Академия управления МВД России

Я. Г. Ищук, Т. В. Пинкевич, Е. С. Смольянинов

ЦИФРОВАЯ КРИМИНОЛОГИЯ

Учебное пособие

Москва • 2021

УДК 343.9
ББК 67.51
И 98

Одобрено редакционно-издательским советом Академии управления МВД России

Рецензенты: *И.В. Ильин*, профессор кафедры административного права Нижегородской академии МВД России, доктор юридических наук, профессор; *Н.Ш. Козаев,* профессор кафедры уголовного права и криминологии Краснодарского университета МВД России доктор юридических наук, доцент.

Ищук Я. Г., Пинкевич Т. В., Смольянинов Е. С.

И 98 Цифровая криминология : учебное пособие. – Москва. : Академия управления МВД России, 2021. – 244 с.

ISBN 978–5–907187–64–1

В учебном пособии рассматриваются наиболее существенные проблемы современной криминологии, в котором наравне с рассмотрением классических вопросов криминологии (преступности, причинного комплекса, личности преступника, предупреждения, виктимологической профилактики, современной зарубежной криминологии) представлен анализ ее частной теории «Цифровая криминология», включающий материалы, определяющие современное направление цифровой криминологии, цифровой преступности, ее видов, криминологических рисков и предупредительного воздействия.

Учебное пособие рекомендовано слушателям, адъюнктам и соискателям при изучении таких учебных дисциплин, как «Организация противодействия преступлениям, совершенным с использованием информационно-телекоммуникационных технологий», «Цифровая криминология» «Уголовная политика». Данное пособие будет интересно профессорско-преподавательскому составу и сотрудникам правоохранительных органов.

УДК 343.9
ББК 67.51

ISBN 978–5–907187–64–1

Авторский коллектив:

Ищук Ярослав Григорьевич, кандидат юридических наук – главы 5, 8, 12.

Пинкевич Татьяна Валентиновна, доктор юридических наук, профессор – главы 1, 2, 3, 4, 6, 7, 10, 11, 13, 14, 15.

Смольянинов Евгений Серафимович, кандидат юридических наук, доцент – глава 9.

Содержание

Предисловие

Криминологическая обстановка, сложившаяся в стране, требует существенной переориентации деятельности, прежде всего, правоохранительных органов на реальное обеспечение криминологической безопасности личности, общества и государства в условиях развития цифровизации общества. Выполнение поставленной задачи требует серьезной подготовки специалистов, которые должны уметь исследовать современное состояние преступности в сфере развития и применения цифровых технологий, выявлять особенности причинного комплекса, анализировать социально-демографические и нравственно-психологические признаки личности преступника, совершившего преступление в сфере цифровых технологий, определять основные направления противодействия названному виду преступности. Такие знания может дать только криминология как социально-правовая общетеоретическая и прикладная наука и дисциплина. Именно она призвана исследовать преступность как социальное явление, определять сущность и формы ее проявления, выявлять закономерности возникновения, существования и изменения преступности.

Это стало основанием к введению в учебный процесс Академии управления МВД России учебной дисциплины «Цифровая криминология», что, в свою очередь, потребовало подготовки учебно-методического обеспечения дисциплины, а в его рамках и учебного пособия «Цифровая криминология».

Основная цель учебного пособия ввести, прежде всего, магистрантов, адъюнктов и соискателей Академии управления МВД России, в сферу криминологических проблем цифровой преступности, показать наравне с классическими и традиционными вопросами, составляющими содержание криминологии, новые проблемы, ранее криминологии неизвестные, расширить круг криминологических знаний профессорско-преподавательского состава, а также практических работников системы МВД России, интересующихся проблемами противодействия преступлениям, совершаемым в сфере цифровых технологий или с их использованием.

Учебное пособие включает материалы по вопросам, связанным с понятием цифровой преступности, анализом ее причинного комплекса, личности преступника, виктимологической профилактики, предупреждению цифровой преступности, уголовной политики в сфере обеспечения цифровой безопасности международных зарубежных основ противодействия цифровой преступности. Особое

внимание уделено характеристике отдельных видов преступлений, совершаемых с использованием цифровых технологий.

В конце каждой главы приведены контрольные вопросы для самостоятельной проверки знаний, а в конце основного текста учебного пособия содержится перечень примерных вопросов для промежуточной аттестации, список рекомендуемой литературы, глоссарий криминологических терминов.

Авторский коллектив настоящего издания будут весьма признателен читателям за замечания и пожелания, направленные на дальнейшее улучшение содержания представленного учебного пособия.

ОБЩАЯ ЧАСТЬ

Глава 1. Социально-правовые предпосылки становления и развития цифровой криминологии как научного направления криминологии

Планируемые результаты освоения темы главы

– **знать** социально-правовые предпосылки становления и развития цифровой криминологии как научного направления криминологии;

– **уметь** применять полученные знания в своей профессиональной деятельности; использовать знания при решении конкретных задач в процессе практических отношений;

– **владеть** навыками криминологической оценки нормативных актов; навыками эффективного осуществления правового воспитания, разработки нормативных правовых актов в соответствие с профилем.

В XVII в. профессор Готфрид Вильгельм Лейбниц писал, что «будущее неизбежно связано со считающими машинами, которые будут настолько совершенны, объективны и эффективны, что смогут беспристрастно взвешивать «за» и «против» и таким образом способствовать, например, судопроизводству»[1]. Беспристрастность в этой сфере искусственного интеллекта уже интересует создателей цифровых платформ и сегодня пророческие предсказания автора сбываются: цифровое будущее становится окружающей нас реальностью; все чаще речь идет о цифровой экономике, цифровых технологиях, цифровой безопасности, и т. д., что делает цифровой мир все более заметной частью нашей реальной жизни. Все это говорит о том, что цифровая экономика, ее потенциал семимильными шагами распространяется во все сферы деятельности современного общества, стремительно вытесняя старый уклад, старое мышление и устаревшие технологии.

С переходом на цифровые платформы и внедрение технологических новшеств произошли серьезные социальные изменения во всем мире, поменялся образ жизни каждого жителя планеты,

[1] *Квашис В. Е.* О новой теории прикладной криминологии: рецензия на учебник В. С. Овчинского «Криминология цифрового мира» // Общество и право. 2018. № 1 (63).

поскольку ежедневно население, дома или на работе, пользуется цифровыми устройствами (компьютеры, смартфоны, бытовая электроника и подобные гаджеты). В медицине внедрение новых цифровых технологий позволило создавать высокотехнологичное оборудование для диагностики, анализа и лечения самых различных болезней, что способствовало новому направлению – цифровой медицины. В финансовой, банковской сфере внедрение цифровых технологий и инновационных финансовых инструментов открывает, безусловно, новые возможности для продвижения не только финансового бизнеса и хозяйственной деятельности, но и оказывает помощь гражданам, делая удобным использования нововведений в банковской сфере в повседневной жизни.

На этом фоне активно развивается рынок цифровых технологий, они активно внедряются в современные управленческие системы как цифровой экономики, так и государственного управления, обороны, безопасности и правопорядка нашей страны.

Их стремительное развитие, направленное на формирование цифрового общества, характеризуется существенными положительными и отрицательными изменениями, происходящими в обществе, процессы внедрения которых не только диктуют новые правила, но и несут в себе огромный потенциал криминологических рисков, о чем свидетельствуют результаты проведенных исследований. Так, по мнению М.М. Бабаева любые инновации «обладали и обладают одновременно как созидательным, так и разрушительным потенциалом»[2]. При этом автор считает, что криминологические «риски современного общества являются фоном, на котором разворачивается, и фактором, который определяет основные направления уголовной политики страны. Область этих рисков – вся наша действительность, все без исключения сферы проявления человеческой активности, которая либо сознательно генерирует, либо допускает возможность наступления неких опасных и вредных последствий»[3].

По этой причине государство «должно страховаться надежными антикриминальными инструментами: как правовыми, так и организационными»[4], поскольку уже сегодня следует гово-

---

[2] *Бабаев М.М.* Риски как компонент детерминационного комплекса преступности // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2018. № 1.

[3] *Там же.*

[4] *Овчинский В.С.* Финансовая «Матрица». Криптовалюта, блокчейн и криминал [Электронный ресурс]. URL: https://info-leaks.ru/archives/21519 (дата обращения: 11.10.2020).

рить о том, что внедрение цифровых технологий способствовало не только росту преступности, но и ее изменению. Так, по мнению Я. И. Гилинского «неопределенность всех социальных процессов в обществе постмодерна, неизбежная переструктуризация видов преступности, появление новых деяний, связанных с развитием новейших технологий, неопределенность политического развития стран, их режимов, от которых в первую очередь зависит конструирование преступности – все это делает непредсказуемым ее дальнейшие тренды»[5].

Совершение преступлений с использованием цифровых технологий уже очевидный факт, количество этих преступлений в последние годы получило широкое распространение. Свидетельством этому является официальная статистика количества зарегистрированных преступлений в России, данные, полученные от организаций, осуществляющих кибербезопасность и мнение их экспертов[6]. Это еще раз убеждает в том, что изменения происходят не только в обществе, меняется и преступность, появились малоизученные способы и средства совершения преступлений, в частности преступления, совершаемые в сфере цифровых технологий или с их использованием (цифровая преступность, преступления в сфере цифровых технологий включают в себя преступления, совершаемые в сфере высоких технологий с использованием информационно-телекоммуникационных технологий). Противодействие этим преступлениям сегодня затруднено, поскольку развитие новой сферы требует подготовки организационно-управленческой правовой основы противодействия этому виду преступности.

В настоящее время уже принят ряд законодательных и нормативных актов, которые составляют правовую основу цифровой экономики[7], организационно-управленческих решений, но необходимо

---

[5] Сборник избранных лекций по криминологии / под ред. д-ра юрид. наук, профессора Т. В. Пинкевич. Москва, 2020. С. 49.

[6] Аналитический материал «Состояние преступности на территории Российской Федерации в условиях пандемии COVID-19 и тенденции ее развития до конца 2020 г. // ВНИИ МВД России, Академия управления МВД России, 2020. С. 77; МВД: ущерб от киберпреступлений в России превысил 210 млрд рублей [Электронный ресурс]. URL: forklog.com (дата обращения: 17.02.2020 г.).

[7] О развитии искусственного интеллекта в Российской Федерации: указ Президента Российской Федерации от 10 октября 2019 г. № 490. Доступ из справ.-правовой системы «КонсультантПлюс»; О безопасности критической информационной инфраструктуры Российской Федерации: федер. закон от 26 июля 2017 г. № 187-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс»; О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса

определение криминологических мер по снижению уровня криминогенности в сфере цифровых технологий и повышению эффективности предупреждения преступлений в сфере цифровых технологий. Однако в настоящее время недостаточно разработан механизм противодействия цифровой преступности,

В сложившейся ситуации требуется научное осмысление проблем противодействия названным явлениям и разработка научно-обоснованных предложений по повышению эффективности деятельности в названной сфере и снижению уровня угроз криминологической безопасности.

С развитием и внедрением в практическую плоскость цифровых технологий становится понятным, что дан как бы научный старт к созданию новых доктрин, научных теорий и развитию новых направлений в научной деятельности значительного количества отраслей не только знаний, но и технологий. В сложившейся ситуации совершенно обоснованно считаем, что необходима разработка теоретических основ цифровой криминологии как самостоятельной отрасли криминологической науки.

Следует признать, что идея развития в криминологии отдельной отрасли «Цифровая криминология» не является новой. Первым в российской криминологической доктрине обратил внимание на эту проблему доктор юридических наук, профессор С. Я. Лебедев. Им сформулированы теоретические основы концепции системного научного знания о технологических инновациях преступности и ее предупреждения под общим термином – киберкриминология[8]. По мнению автора, киберкриминология

Российской Федерации: федер. закон от 18 марта 2019 г. № 34-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс»; О безопасности: федер. закон от 28 декабря 2010 г. № 390. Доступ из справ.-правовой системы «КонсультантПлюс»; О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации: федер. закон от 2 августа 2019 г. № 259-ФЗ. Доступ из справ.-правовой системы «Консультант плюс»; О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: указ Президента Российской Федерации от 9 мая 2017 г. № 203. Доступ из справ.-правовой системы «КонсультантПлюс»; О Стратегии национальной безопасности Российской Федерации: указ Президента Российской Федерации 31 декабря 2015 г. № 683. Доступ из справ.-правовой системы «КонсультантПлюс»; Об утверждении программы «Цифровая экономика Российской Федерации»: распоряжение Правительства Российской Федерации от 28 июля 2017 г. № 1632-р. Доступ из справ.-правовой системы «КонсультантПлюс» (программа утратила силу, как выполнившая свою функцию); и др.

[8] *Шестаков Д. А., Дикаев С. У., Данилов А. П.* Летопись Санкт-Петербургского международного криминологического клуба. Год 2014 // Криминология: вчера, сегодня, завтра. 2015. № 1 (36). С. 72–95.

должна стать теоретической и прикладной отраслью криминологической науки и специальной инновационно-технологической практики социально-правового контроля над киберпреступностью. Создатель концепции утверждает, что достойное правоохранительное место должен занять соответствующий уголовно-правовой ресурс[9]. При этом было предложено «целенаправленное и масштабное объединение профессиональных научно-аналитических потенциалов экономистов, юристов и информационных технологов вокруг формирования адекватной современным цифровым угрозам безопасности и оптимальной по своим экономическим, правовым и информационно-технологическим ресурсам новой цифровой модели обеспечения безопасности личности, общества, государства»[10].

С данной концепцией, содержащей все основные разделы современного теоретико-методологического фундамента отечественной криминологии, интерпретированного к системе познания современной и будущей преступности, а также процессов ее предупреждения, связанных с инновационными технологиями, культивируемыми в виртуальном (цифровом) информационном пространстве, научное сообщество познакомилось в 2014 г. В настоящее время доктор юридических наук, профессор С.Я. Лебедев предлагает «идею разработки самостоятельного цифрового уголовно-правового сегмента социально-правового контроля над преступностью в киберпространстве»[11].

Рассуждая о названной концепции, предложенной С.Я. Лебедевым В.Ф. Джафарли в своем докладе «О созвучности тезиса «цифровой безопасности – цифровой уголовно-правовой ресурс» теории криминологической безопасности в сфере информационных технологий» ее поддерживает и рассуждая о ее значимости, как бы дополняя ее указывает, что «в определенной мере реализация тезиса «Цифровой безопасности – цифровой уголовно-правовой ресурс» может быть осуществлена через формирование и развитие системы криминологической безопасности в сфере информационных технологий (системы кри-

---

[9] *Лебедев С.Я.* Цифровая безопасность – цифровой уголовно-правовой ресурс // Криминология: вчера, сегодня, завтра. № 4 (55), 2019. С. 18–19.

[10] Из выступления С.Я. Лебедева на заседании Санкт-Петербургского международного криминологического клуба 6 декабря 2019 года «Право, цифровизация и безопасность в преступностиведческом поле (возвращаясь к теме)» [Электронный ресурс]. URL: http://www.criminologyclub.ru/home/3-last-sessions/373-2019-12-08-11-57-27.html (дата обращения: 08.12.2019).

[11] *Там же.*

минологической кибербезопасности). В свою очередь, данный процесс сопряжен с оформлением трех ресурсов – уголовно-правового, криминологического и информационно-технологического, дальнейшее развитие которых должно носить исключительно комплексный характер, происходить путем постоянного взаимодействия»[12].

Значительный вклад в исследование преступности цифрового мира внесен доктором юридических наук В.С. Овчинским. Им подготовлен огромный массив информационно-аналитического материала, который позволяет изучить проблемы цифровизации противодействия цифровой преступности в зарубежных странах и на международном уровне.

В 2018 г. вышел в свет подготовленный им учебник для магистров «Криминология цифрового мира» в предисловии, к которому, автор указывает: «Криминология цифрового мира представляет собой, с одной стороны, часть общей науки криминологии, на которую распространяется традиционное учение о причинах преступности, личности преступника, мерах предупреждения преступлений. С другой стороны, учитывая специфический характер самого цифрового мира, действующей в нем преступности и факторов, ее детерминирующих, криминология цифрового мира может рассматриваться как самостоятельная наука, предполагающая также и самостоятельную учебную дисциплину»[13]. Его научные взгляды были расширены в работах, которые содержат анализ развития отдельных цифровых технологий и их влияние на рост преступности, представлены и результаты исследования криминологических угроз и рисков, а также меры эффективного противодействия преступности в названной сфере[14].

---

[12] *Джафарли В. Ф.* О созвучности тезиса «цифровой безопасности – цифровой уголовно-правовой ресурс» теории криминологической безопасности в сфере информационных технологий // Криминология: вчера, сегодня, завтра. № 4 (55), 2019.

[13] *Овчинский В.С.* Криминология цифрового мира : учебник для магистратуры / В.С. Овчинский. Москва, 2018.

[14] *Овчинский В.С.* Виртуальный щит и меч: США, Великобритания, Китай в цифровых войнах будущего («Коллекция Изборского клуба»). Москва, 2018; *Овчинский В.С.* Иностранные боевики-террористы. Иногда они возвращаются. («Коллекция Изборского клуба»). Москва, 2019; *Ларина Е.С., Овчинский В.С.* Искусственный интеллект. Большие данные. Преступность // («Коллекция Изборского клуба»). Москва, 2018; *Ларина Е.С.* Роботы-убийцы против человечества. Кибер-апокалипсис сегодня / Е.С. Ларина, В.С. Овчинский. Москва, 2018; *Ларина Е.С.* Искусственный интеллект. Этика и право. Судья с искусственным интеллектом / В.С. Овчинский, Е.С. Ларина / («Коллекция Изборского клуба»). Москва, 2019, и др.

Следует согласиться с мнением А. И. Долговой, что развитие новых отраслей криминологии не означает рождения соответствующих новых наук[15], но новая отрасль знаний повлияет и на развитие криминологии в целом. Это обусловлено тем, что цифровая экономика отличается от реальной, поскольку она существует только в виртуальном мире, ее уникальной особенностью являются виртуальные товары, виртуальная валюта и электронные деньги. Она полностью зависит от развития цифровых технологий, телекоммуникационных сетей и компьютерной техники и несет в себе значительный потенциал криминологических угроз личности, обществу и государству. Следовательно, будут изменены не только особенности сбора эмпирического материала и его анализа, изучение причинного комплекса и личности преступника с использованием технологий искусственного интеллекта, больших данных и иных цифровых технологий, но будут изменена и система криминологической цифровой безопасности.

Все вышеизложенное дает основание полагать, что цифровая криминология – самостоятельное научное направление (отрасль научного познания), изучающее криминогенное влияние развития цифровой экономики и цифровых технологий на социальные процессы, происходящие в обществе. Она является частью общей криминологии, которая требует надлежащей компетенции, включающей не только знание закономерностей преступности, анализа ее современного состояния, владение методикой ее сбора и создания банка эмпирических данных, умение формулировать гипотезы перспективных направлений исследований, иметь достаточную научную эрудицию, обладать навыками обобщения и интерпретации структурных и динамических распределений[16], но и иного уровня получения знаний, касающихся противодействия преступности в сфере цифровой экономики.

Противодействие цифровой преступности будет эффективным в том случае, когда будет осуществлено «целенаправленное и масштабное объединение профессиональных научно-аналитических потенциалов экономистов, юристов и информационных технологов вокруг формирования адекватной современным цифровым угрозам безопасности и оптимальной по своим экономическим, правовым

[15] *Долгова А. И.* Теоретические проблемы криминологии как науки // Предупреждение преступности. 2001. № 1. С. 49.

[16] *Клейменов И. М.* Сравнительная криминология: криминализация, преступность, уголовная политика в условия глобализации: дис. ... д-ра юрид. наук. Омск, 2015. С. 25.

и информационно-технологическим ресурсам новой цифровой уголовно-правовой модели обеспечения безопасности личности, общества, государства...»[17]. При этом цифровая криминология научно обеспечивает реализацию важнейшего элемента указанного обеспечения безопасности – предупреждения преступлений.

Контрольные вопросы

1. Назовите социальные предпосылки становления и развития цифровой криминологии.
2. Назовите правовые предпосылки становления и развития цифровой криминологии.
3. Выберите правильный вариант ответа: цифровая криминология – это: а) научное направление; б) научная теория; в) частная теория криминологии.
4. Перечислите особенности, которые позволят развиваться новому научному направлению – цифровой криминологии.

[17] *Лебедев С.Я.* Цифровой безопасности – цифровой уголовно-правовой ресурс // Криминология: вчера, сегодня, завтра. 2019. № 4 (55). С. 23.

Глава 2. Цифровая преступность и ее виды

Планируемые результаты освоения темы главы

– **знать** понятие цифровой преступноти, как социального явления; понимать характерные ее особенности; виды цифровой преступности;

– **уметь** применять свои знания для понимания закономерностей и тенденций развития цифровой преступности; при анализе современного состояния цифровой преступности использовать статистические показатели; ориентироваться в особенностях определения латентной преступности и социальных последствий;

– **владеть** терминологией цифровой преступности; навыками для организации и проведения криминологических исследований; прогнозирования цифровой преступности, планирования профилактических мероприятий.

2.1. Понятие и особенности цифровой преступности

Существенным фактором, затрудняющим определение цифровой преступности, является и так называемая юрисдикционная дилемма, поскольку в разных странах данный термин понимается и определяется по-разному. Кроме того, отсутствуют и надлежащие конкретные статистические данные о совершенных преступлений названного вида. Та же проблема присутствует и в России, в которой понятие «цифровая преступность» в настоящее время на законодательном уровне отсутствует. И для российской криминологической науки понятие «цифровая преступность» является новым и почти не исследованным. Есть опыт зарубежных ученых в исследовании киберпреступности, но он тоже не дает полной картины и определения тем преступлениям, которые совершаются в сфере цифровых технологий или с их использованием.

Известно, что термин «компьютерная преступность» впервые был использован в одном из докладов Стэнфордского исследовательского института. Позже в статьях по киберпреступности была принята следующая классификация: компьютер как субъект преступления; компьютер как объект преступления; или компьютер как инструмент (четвертый вариант, предложенный в 1973 году, – компьютер как символ – по-видимому, вышел из употребления в 1980-х годах).

Так, были выработаны два определения киберпреступности в узком и широком понимании. При этом, в первом случае, кибер-

преступность рассматривается как любое противозаконное поведение в форме электронных операций, которые направлены на нарушение безопасности компьютерных систем и данных, которые ими обрабатываются. В широком смысле рассматривают любое противозаконное поведение, которое осуществляется с использованием компьютерной сети или посредством компьютерных систем. Как свидетельствуют материалы судебной практики к таковым следует отнести незаконное владение, предложение или распространение информации посредством компьютерной системы или сети[18].

Впервые проблемы предупреждения компьютерных преступлений рассматривались на восьмом Конгрессе по предупреждению преступности и обращению с правонарушителями, состоявшегося в 1990 г. ООН активно занимается рассмотрением различных аспектов, связанных с использованием компьютеров. В 1992 году ОСЭР подготовил «Директивы по проблеме безопасности информационных систем». Они впоследствии были пересмотрены и 25 июля 2002 г. приняты в качестве Рекомендаций Совета ОЭСР «Директивы по проблеме безопасности информационных систем и сетей: формирование культуры обеспечения безопасности»[19].

Определение киберпреступности было дано в 2000 году в ходе работы сессии десятого Конгресса ООН по предупреждению преступности и уголовному правосудию. Было признано, что компьютерное преступление касается любого преступного деяния, «которое может совершаться с помощью компьютерной системы или сети, в рамках компьютерной системы или сети или против компьютерной системы или сети. В принципе, оно охватывает любое преступление, которое может совершаться в электронной среде»[20].

Но уже в рамках одиннадцатого Конгресса ООН по предупреждению преступности и уголовному правосудию (2005 г.) было предложено «по-иному сформулировать эту концептуальную модель, рассматривая преступления, связанные с использованием компьютеров, как запрещаемое законом и/или судебной практикой пове-

---

[18] Основы борьбы с киберпреступностью и кибертерроризмом: хрестоматия [Электронный ресурс] / сост. В.С. Овчинский. Москва, 2017. URL: http://cybersafetyunit.com (дата обращения: 01.12.2020).

[19] Обзор: Директива ОЭСР по проблеме безопасности информационных систем и сетей: формирование культуры обеспечения безопасности [Электронный ресурс]. URL: https://www.oecd.org/sti/ieconomy/15582276.pdf (дата обращения: 23.08.2020).

[20] Справочный документ для семинара-практикума по преступлениям, связанным с использованием компьютерной сети [Электронный ресурс]. URL: file://C:/Users/Ekaterina/Downloads/A_CONF.187_10-RU.pdf. С. 4 (дата обращения: 03.10.2020).

дение, которое a) направлено собственно на компьютерную сферу и коммуникационные технологии; b) включает использование цифровых технологий в процессе совершения правонарушения; c) включает использование компьютера как инструмента в процессе совершения иных преступлений, и, соответственно, компьютер выступает при этом как источник электронных процессуальных доказательств»[21].

Представлено понятие и в Соглашении Шанхайской организации сотрудничества и определяется оно как «информационная преступность», под которой следует понимать «использование информационных ресурсов и (или) воздействие на них в информационном пространстве в противоправных целях»[22].

20–27 апреля 2020 г. в г. Киото должен был состояться четырнадцатый Конгресс ООН по предупреждению преступности и уголовному правосудию. В материалах Семинара-практикума «Современные тенденции в области преступности, последние изменения и новые решения, в частности, использование современных технологий как средства совершения преступления и инструмента борьбы с преступностью» вновь предполагается обсудить проблемы использования современных технологий при совершении преступлений. Причем следует обратить внимание, что в предварительных материалах Конгресса понятия «киберпреступность», «компьютер» уже практически не используются. Речь идет о современных информационных и цифровых технологиях[23].

В Конвенции Совета Европы (Будапештская конвенция) так же отсутствует определение киберпреступности, но в этом документе этот вид преступности относится к компьютерным преступлениям и дают их классификацию:

– преступления против конфиденциальности, целостности и доступности компьютерных данных или систем;

– правонарушения, связанные с использованием компьютерных средств;

---

[21] Предварительные итоги Одиннадцатого Конгресса Организации Объединенных Наций по предупреждению преступности и уголовному правосудию. Бангкок, 18–25 апреля 2005 года [Электронный ресурс]. URL: http://www.crime-research.ru/analytics/crime_bangkok (дата обращения: 20.12.2020).

[22] Соглашение между Правительствами государств – членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности (заключено в г. Екатеринбурге 16.06.2009). Доступ из справ.-правовой системы «КонсультантПлюс».

[23] Руководство для дискуссий. Четырнадцатый Конгресс ООН по предупреждению преступности и уголовному правосудию [Электронный ресурс]. Киото. Япония, 20–27 апреля. URL: //A/conf/234/PM.1. C. 50–56.

– правонарушения, связанные с содержанием компьютерных данных.

На постсоветском пространстве определение компьютерного преступления дано в Соглашении о сотрудничестве государств – участников Содружества СНГ в борьбе с преступлениями в сфере компьютерной информации, в котором дается определение «преступления в сфере компьютерной информации», которое представляет собой «уголовно наказуемое деяние, предметом посягательства которого является компьютерная информация». При этом, к компьютерной информации названный документ относит информацию, находящуюся в памяти компьютера, на машинных или иных носителях в форме, доступной восприятию ЭВМ, или передающаяся по каналам связи[24]. Среди них присутствуют составы, которые не учтены в положениях Будапештской конвенции, например «распространение с использованием информационно-телекоммуникационной сети Интернет или иных каналов электрической связи материалов, признанных в установленном порядке экстремистскими или содержащих призывы к осуществлению террористической деятельности или оправданию терроризма». Но в 2018 г. в Душанбе подготовлен новый документ (он пока не вступил в силу), который посвящен борьбе стран СНГ с преступлениями в сфере информационных технологий, фактически же речь по-прежнему идет о преступлениях в сфере компьютерной информации.

В Модельном уголовном кодексе государств СНГ также установлена ответственность за компьютерные преступления[25].

Таким образом, в международных актах понятие «цифровая преступность» практически отсутствует, большинство международных актов использует термин «компьютерное преступление», под которым понимается любое деяние, в котором инструментом, целью или местом преступных действий являются компьютеры, компьютерные сети, а также цифровые технологии.

В законодательстве зарубежных стран употребляются, не только термины «компьютерные преступления», но и «электронные

---

[24] Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации» (Заключено в г. Минске 01.06.2001) // Бюллетень международных договоров. 2009. № 6. С. 12–17.

[25] Модельный уголовный кодекс для государств – участников Содружества Независимых Государств. Рекомендательный законодательный акт (принят в г. Санкт-Петербурге 17 февраля 1996 г. Постановлением 7–5 на 7-ом пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ [Электронный ресурс]. URL: http://iacis.ru/.

средства связи», «информационные технологии» или «преступления в сфере высоких технологий».

В Российской Федерации данной теме посвящен ряд диссертационных исследований, но в большей своей части он посвящен преступлениям, совершаемым с использованием информационно-телекоммуникационных сетей и «Интернет», к которым авторы относят группу преступлений в сфере компьютерной информации.

Последние несколько лет были проведены исследования этих преступлений, но перечень уголовно-правовых норм просто был расширен. В настоящее время в уголовном законе использование признака «с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет»)» предусмотрено в 19-ти нормах Особенной части УК РФ. Неслучайно с начала 2017 г. отдельной строкой стали выделяться деяния, совершаемые с использованием компьютерных и телекоммуникационных технологий в уголовной статистике при учете преступлений экономической направленности. Однако при квалификации других деяний, посягающих на самые различные объекты уголовно-правовой охраны, использование сетей телекоммуникации не учитывается вовсе и не может быть учтено, ввиду отсутствия конструктивных признаков состава преступления. Но если ранее для изучения вышеперечисленных норм достаточно было раскрыть понятие «преступность с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет»)», то сегодня, с развитием цифровых технологий, на наш взгляд, необходимо рассматривать данную проблему шире, так как рост технических возможностей обусловил возможность неправомерных действий посредством цифровых технологий не только в сфере информации, но и в иных сферах человеческой жизнедеятельности.

В связи с вышеизложенным, можно с уверенностью утверждать, что понятия «цифровая преступность» пока российской криминологической доктрине не известно, предпринимаются только попытки к его исследованию. В то же время в сложившейся криминогенной обстановке следует говорить о том, что понятие «цифровая преступность» шире понятия «киберпреступность», поскольку цифровые технологии главным образом используются в вычислительной цифровой электронике (в том числе компьютеры и использование информационно-телекоммуникационных сетей (включая сеть Интернет), в различных областях электротехники, таких как игровые автоматы, робототехника, автоматизация, измерительные приборы, радио и теле-

видение, и многие другие цифровые устройства и прочие средства сбора, хранения, анализа информации и обмена ею в цифровом формате. Более того, распространение вредоносных программ может осуществляться не только через компьютер и Интернет, но также и через технологии MMS, Bluetooth и другие цифровые программы, в рассматриваемой ситуации противоправное деяние в полной мере не будет подпадать под понятия «интернет-преступления» или «компьютерная преступность». Как видим данный вид преступности включает более широкий диапозон противоправных действий, в том числе совершаемых как в сфере цифровых технологий, так и с их использованием, в том числе и в виртуальной среде, дополняющей нашу реальность. Таким образом, цифровая преступность – это социальное противоправное явление, включающее в себя совокупность преступлений, совершаемых в сфере цифровых технологий или с их использованием, в том числе включая незаконное завладение и предложение или распространение информации в информационно-телекоммуникационных сетях и в виртуальной среде, дополняющей реальность. Следует обратить внимание на то, что подобный подход позволяет рассмотреть более широкий круг составов противоправных деяний, совершаемых в рассматриваемой области. Примером этих преступлений может служить использование при совершении преступлений виртуальной валюты (криптовалюты).

Особенность цифровых преступлений заключается в том, что с развитием цифровых технологий преступность изменилась и большая ее часть совершается в виртуальной среде.

Теоретическая и практическая значимость классификации состоит в том, что она позволяет группировать изучаемые объекты в зависимости от потребностей теории и практики, обеспечивая тем самым решение многообразных теоретических и прикладных задач. Она позволяет уточнить уровень и объем знаний о предмете исследования и определить наиболее эффективные пути использования этих знаний на практике.

Итак, исследовав особенности цифровой криминологии, цифровой экономики и цифровых технологий, можно в качестве критерия классификации рассмотреть, с одной стороны, разделение на виды преступлений, с учетом имеющейся классификации, согласно уголовного законодательства и эта классификация всем известна и показать особенности этих преступлений (около 280 статей), а с другой стороны, классифицировать по направлениям развития цифровой экономики, в основу которых положены сквозные

цифровые технологии, по сферам их внедрения, а можно классифицировать по категориям преступлений.

Итак, выделяют три вида цифровых преступлений. К таковым следует отнести две категории деяний, которые совершены:

– в отношении развивающихся цифровых технологий (нейротехнологии и искусственного интеллекта, робототехники; оборота виртуальной валюты (криптовалюты); использование IoT (интернет вещей); технологий больших данных; квантовых технологий, в том числе цифровой электронике (кроме компьютеров), в различных областях электротехники, таких как игровые автоматы, робототехника, автоматизация, измерительные приборы, радио и телевидения, и многие другие цифровые устройства и прочие средства сбора, хранения, анализа информации и обмена ею в цифровом формате) или с их использованием;

– с использованием компьютерных устройств и программ как:

а) средства совершения преступления (пропаганда ненависти и вражды, экстремизма и террористической деятельности, незаконный оборот наркотиков и оружия, легализация (отмывание) преступных доходов, незаконные азартные игры, распространение порнографии, мошенничество);

б) орудие совершения преступления (для изготовления поддельных денег, ценных бумаг или документов);

в) предмет совершения преступления (несанкционированное использование компьютерной системы, несанкционированное распространение данных, незаконное проникновение в компьютер (взлом), распространение компьютерных вирусов).

К таковым следует отнести:

– **хакинг** – внесение изменений (взлом защиты компьютерной сети, отключение сайтов и пр.) в программном обеспечении для достижения определенных целей, отличающихся от целей создателей программ, очень часто изменения являются вредоносными);

– **кардинг** – кражи баз данных кредитных карт с полной информацией о владельце, отмывание денег и получение незаконно купленного товара;

– **фишинг-атаки** – это вид интернет-мошенничества, построенный на принципах социальной инженерии (хищение с использованием электронных средств доступа персональных данных, номеров кредитных карт, паролей и персональных данных с целью дальнейшего их использования для хищения денежных средств, которые в дальнейшем невозможно оспорить).

Работает фишинг и через перенаправление пользователей на поддельные сетевые ресурсы, являющиеся полной имитацией настоящих.

По данным проведенных исследований 80 % успешных хакерских атак начинается с фишинга (а по некоторым данным 95 %); 10 % сигналов тревоги в SOS связано с фишинговыми атаками, рейтинг успешных кликов на фишинговые ссылки – 21 %, Рейтинг загрузки/запуска вредоносных приложений 11 %[26].

К третьему виду классификации по сферам применения цифровых технологий можно отнести преступления, совершенные в сферах электронной коммерции, цифровой логистики, цифровой медицины, цифрового страхования, цифровой недвижимости, интеллектуальной собственности, Интернета, вещей (IoT) и др.

Данное деление условно, поскольку нет еще достаточных данных, которые бы позволили возвести эту классификацию в разряд обязательных.

[26] Чеклист для борьбы с фишингом [Электронный ресурс]. URL: https://habr.com/ru/company/cisco/blog/465085/ (дата обращения: 07.04.2021).

2.2. Цифровая организованная преступность и ее особенности

Организованная преступность по-прежнему крайне негативно влияет на состояние национальной безопасности России, активно внедряясь не только в экономическую деятельность, но и в органы государственной власти и управления.

Современная организованная преступность активно использует в своей деятельности цифровые технологии, что и способствовало изменению ее структуры, в которой теряется взаимосвязь и личное взаимодействие ее участников, все большее распространение получает блочно-сетевая организованная преступность, в том числе и трансграничная[27].

Ситуация осложняется тем, что у преступников появилась возможность не только использовать новые средства и способы для совершения преступлений, но и избегать уголовной ответственности, поскольку анонимность и безопасность организаторов совершения преступлений, в силу использования новейших цифровых технологий, позволят им осуществлять длительно преступную деятельность и использовать их в качестве контрмер правоохранительным органам. По мнению В.С. Овчинского, организованные преступные группы «весьма разнообразны по своей организационной структуре, функционалу и составу. Они варьируются от крупных традиционных иерархических ОПГ до гибких устойчивых сетевых структур и небольших высокотехнологичных групп, ориентированных на конкретные виды преступности»[28].

Так, на международном уровне, в пункте 3 статьи 27 Конвенции об организованной преступности предусмотрено, что государства должны стремиться сотрудничать и совместными усилиями противодействовать транснациональной организованной преступности, используя при этом современные технологии. Все это совершенно верно. И, действительно, призыв об использовании цифровых технологий для противодействия преступности, в том числе и организованной преступности, видимо своевременен. Однако организованная преступность активно внедряет цифровые технологии в свою преступную деятельность, что и послужило основой изменения подходов к подготовке ряда тяжких и особо тяжких преступлений в сфере экономической деятельности.

---

[27] *Овчинский В.С.* Криминология цифрового мира. Москва, 2018. С. 209.

[28] *Там же.*

Вместе с трансформацией цифровой экономики произошла трансформация экономической, организованной преступности, изменилась и преступность террористической направленности. Все чаще они стали совершаться с использованием информационно-телекоммуникационных технологий[29], то есть большая их часть совершается в виртуальной среде, что не позволяет своевременно предотвращать, пресекать такие преступления и выявлять лиц, причастных к их совершению.

Кроме того, ими активно используются и коррупционные связи. Самый высокий уровень коррупции, по мнении экспертов, «связан с киберпреступностью в финансовой и торговой сферах. Практически совершение любого крупного киберпреступления в онлайн банкинге или торговле поддерживается преступными инсайдерами изнутри компании»[30], а иногда в их качестве используются и бывшие сотрудники финансовых учреждений и структур, хорошо осведомленные о системе безопасности.

В настоящее время организованной преступностью предпринимаются попытки к тотальному контролю над электронной торговлей, маркетингом, деньгами, банкингом, страховыми услугами.

Следует отметить, что этот вид организованной преступности, как правило, состоит из представителей нескольких стран. Примером может служить преступная деятельность в сфере незаконного оборота наркотиков. Этот криминальный вид деятельности является высоко прибыльным и высоко латентным. В последние годы изменились особенности транспортировки и с развитием цифровых технологий организованные преступные группы в целях контрабанды уже стали использовать инновационные технологии, в том числе дронов и роботов.

Помимо наркотрафика, преступные формирования названного типа контролируют организованную педофилию и незаконное изъятие, хранение, транспортировку, изъятие и использование органов и тканей человека для трансплантации, осуществляют незаконную торговлю оружием, торговлю людьми, и пр. В последние годы участились случаи использования криптовалюты при оплате помимо названных заказных преступлений, приобретения и распространения порнографических материалов.

Причина, по которой они используют криптовалюту, заключается в том, что она обеспечивает анонимность транзакций, кото-

---

[29] За последние 5 лет возросло в 25 раз (в 2019 года – 294 тыс.), особенно с учетом низкой их раскрываемости (25 %). В первом полугодии 2020 года негативная тенденция лишь усилилась. Зафиксирован рост на 92 % (225 тыс.), чем в 2019 г. за аналогичный период [Электронный ресурс]. URL: https://genproc.gov.ru/smi/news/genproc/news-1880616.

[30] *Овчинский В. С. Там же.*

рая гарантирована несколькими уровнями шифрования киберкошельков и мгновенной скоростью перемещения платежей (от 15–20 секунд, например Dash, до 5–10 минут у Bitcoin).

Направление преступной деятельности этого вида организованной преступности распространяется на мошенничество и вымогательство, совершаемые в сфере оборота виртуальных денег. При этом факты этих преступлений в IT-сфере будут только увеличиваться.

Особое место в деятельности организованной преступности отведено преступлениям, совершаемым в финансово-кредитной сфере. Уже сегодня следует говорить о росте преступлений в сфере финансовых пирамид и оборота криптовалюты. Сегодня функционирует множество холдингов и инвестиционных площадок, которые осуществляют свою деятельность путем привлечения инвесторов, деятельность которых заключается в приеме в доверительное управление криптовалюты путем торгов на бирже и бонусной системы поощрений, выплате процентов инвесторам. Здесь прослеживается причастность к этой деятельности представителей организованных преступных формирований.

Еще одно направление, которое является лакомым кусочком для организованной преступности в сфере цифровых технологий – это технологии «Больших данных» («big data»), огромный объем неоднородной и быстро поступающей цифровой информации, которую невозможно обработать традиционными инструментами», но ее можно использовать во многих сферах жизнедеятельности общества, в том числе и в преступных целях[31].

Контрольные вопросы

1. Раскройте особенности цифровой преступности.
2. Определите признаки цифровой преступности.
3. Назовите преступления, совершаемые организованными преступными формированиями с использованием цифровых технологий.
4. Назовите типичные причины и условия преступлений, совершаемых с использованием цифровых технологий.

[31] Сотрудниками Управления «К» МВД России совместно с оперативниками отдела «К» ГУ МВД России по Нижегородской области и УФСБ России по Нижегородской области пресечена деятельность злоумышленников, осуществлявших несанкционированный доступ к компьютерам руководителей крупных государственных и коммерческих организаций с целью получения конфиденциальной информации [Электронный ресурс]. URL: https://xn–b1aew.xn–p1ai/news/item/ (дата обращения: 15.12.2020).

Глава 3. Современное состояние цифровой преступности в России

Планируемые результаты освоения темы главы

– **знать** количественные и качественные показатели преступности в сфере развития и использования цифровых технологий, причины и условия, способствующие их совершению, и направления их предупреждения;

– **уметь** применять свои знания при характеристике современного состояния преступности в сфере развития и использования цифровых технологий; ориентироваться в особенностях определения латентной преступности, социальных последствий и причинного комплекса;

– **владеть** терминологией преступности в сфере развития и использования цифровых технологий; навыками организации и проведения криминологических исследований, прогнозирования этого вида преступности, планирования профилактических мероприятий.

3.1. Особенности и проблемы противодействия цифровой преступности

Рассматривая современное состояние цифровой преступности, необходимо отметить, что большая часть сквозных цифровых технологий, в настоящее время находится только в стадии развития, некоторые из них уже не только активно развиваются, но и используются в России. Так, например, технология «блокчейн» активно используется на территории России, а также широкое распространения, о чем свидетельствуют результаты проведенного социологического исследования, получил такой финансовый актив, как виртуальная валюта (криптовалюта), а его оборот, рост соответствующих транзакций, ежедневно увеличивается. Но развитие остальных цифровых технологий уже «не за горами» и совершение преступлений с их использованием уже очевидный факт. Преступления могут совершаться не только в сфере оборота цифровых финансовых активов (в том числе и виртуальной валюты (криптовалюты), но и в сфере развития и использования технологии больших данных, искусственного интеллекта, производственных технологий и т. п.

Анализ криминальной ситуации, сложившейся в сфере внедрения и использования цифровых технологий, свидетельствует о том, что преступления имеют тенденцию к росту. Так, например, только за 2019 г. в этой сфере было зарегистрировано 294 тыс. преступлений, что на 70 % больше, чем в 2018 г. При этом 98, 4 тыс. зарегистрированных преступлений относится к категории тяжких и особо тяжких преступлений. Ущерб от хищений, совершенных с использованием цифровых технологий в 2019 г., по данным МВД России, составил более 10 млрд рублей[32], а раскрываемость этих преступлений составила 20, 5 %[33]. Так, по данным Национального отделения ФБР, от 85 % до 97 % компьютерных посягательств даже не выявляются[34]. По оценкам других экспертов, латентность этих преступлений в США достигает 80 %, в Великобритании – 85 %, в ФРГ – 75 %, в России – более 90 %[35].

За десять месяцев 2020 г. рост исследуемых преступлений составил 75,1 % и было зарегистрировано 420,7 тыс. преступлений, из них количество особо тяжких и тяжких преступлений увеличилось, по сравнению с предыдущим периодом на 84,9 % (216,4 тыс.). При совершении этих преступлений использовались или применялись: сети «Интернет» (243,6 тыс.), средства мобильной связи (181, 2 тыс.), расчетные (пластиковые) карты (161,4 тыс.) компьютерная техника (23,8 тыс.), программные средства (8,2 тыс.), фиктивные электронные платежи (1,1 тыс.). Большая часть из них совершена против собственности как юридических, так и физических лиц в финансовой и банковской сфере, в сфере незаконного оборота наркотиков и пр.

Широкое распространение получили преступные деяния с использованием банковских карт. Так, более 80 % зарегистрированных преступлений в названной сфере совершены против собственности, в основном это кражи и мошенничество. Так, распространение мошенничество получило при внесении изменений в единый государственный реестр фиктивных сведений юридических

---

[32] Обзор: МВД: ущерб от киберпреступлений в России превысил 210 млрд рублей [Электронный ресурс]. URL: forklog.com (дата обращения 17.02.2020 г.).

[33] Обзор: Краткая характеристика состояния преступности в Российской федерации за январь – декабрь 2019 года: МВД России [Электронный ресурс]. URL: https://мвд.рф/reports/item/19412450 (дата обращения: 17.02.2020 г.).

[34] *Айков Д.* Компьютерные преступления: Руководство по борьбе с компьютерными преступлениями / Д. Айков, К. Сейгер, У. Фонсторх; пер. с англ. В.И. Воропаева и Г.Г. Трехалина. Москва: Мир, 1999.

[35] *Волеводз А.Г.* Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. Москва, 2002; *Андреев Б. В., Пак П. Н., Хорст В.П.* Расследование преступлений в сфере компьютерной информации. Москва, 2001.

лиц и индивидуальных предпринимателей, в результате которых злоумышленники получили возможность завладеть имуществом, активами физических и юридических лиц, в том числе с государственной долей уставного капитала.

Проблема раскрываемости этих преступлений заключается в том, что большая часть этих преступлений совершается в виртуальной среде, что не позволяет своевременно выявить лиц, причастных к свершению таких преступлений.

Следует отметить, что цифровые преступления, по своей сути, малоизучены и имеют высокий уровень латентности, что обусловлено, с одной стороны «отсутствием современной методической базы исследования этого вида деяний, недостаточными знаниями IT-технологий, изменением способов совершения преступлений и пр. Действительно, в настоящее время, преступления могут совершаться в виртуальной среде, не выходя из своего дома или офиса и сохраняя анонимность»[36].

Особую тревогу вызывают хакинг, кардинг и современный фишинг. Чаще всего объектами хакерских атак становится промышленность, в 28,9 % случаев, и правительственные учреждения, в 25 % случаев. Этот показатель свидетельствует о том, что преступные формирования сегодня стремятся владеть всей информацией о развитии новых технологий, их внедрении в промышленность, о принятии новых законов и иных нормативных актах, а также получать информацию о деятельности правительства.

Анализ типов атак, проведенный Центром мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (inCERT), направленных на организации кредитно-финансовой сферы показал, что в первом полугодии 2019 года семь криптобирж, включая крупнейшие Bithumb и Binance, пострадали от крупных взломов, потеряв при этом десятки миллионов долларов средств пользователей. Позже Сингапурская криптобиржа Bitrue официально заявила о краже токенов XRP на сумму $3.9 млн и токенов Cardano (ADA) на сумму $225,000. Таким образом, вместе с новым взломом, число успешных хакерских атак в 2019 году выросло до 8, что вновь выводит на первый план вопросы безопасности. Стремительный рост котировок делает кошельки криптобирж невероятно привлекательными для хакеров, поэтому в дальнейшем ситуация будет только ухудшаться.

---

[36] *Конев Д.А.* Криминологическая безопасность и ее обеспечение в сфере цифровых технологий: постановка проблемы // Криминальная ситуация в России и антикриминальное законодательство: проблемы криминологической обусловленности закона. Москва, Российская криминологическая ассоциация. 2020.

По мнению представителей компании «Лаборатория Касперского», результаты проведенного ими исследования, в котором приняли участие индустриальные организации почти всех стран мира, включая Россию, пришли к выводу, что за последний год более 50 % промышленных компаний в мире пострадала от одной до восьми хакерских атак. При этом были затронуты критически важные инфраструктуры или автоматизированные системы управления технологическими процессами. Представителями таких организаций было потрачено в течение года на устранение последствий от таких атак до 420 тыс. долларов США. Не стало неожиданностью для промышленных предприятий и компаний, как свидетельствуют результаты опросов, вероятность пострадать от хакерских атак. Их допускают три четверти компаний, при этом, по их мнению, (83 %), к таким инцидентам в их промышленных инфраструктурах они хорошо подготовлены. В настоящее время компании больше всего опасаются возможности заражения вредоносным программным обеспечением, так как пострадавшие от хакерских атак (53 %) подтвердили случаи столкновения с различным вредоносным программным обеспечением[37].

В начале 2020 г. компанией Group-IB зафиксирован фишинг шпионской программы HawkEye с темой Free face Mask. Письмо было отправлено якобы от менеджера китайской компании GALAXY ELECTRONIC INDUSTRIAL, а получателями были российские компании, в том числе из сферы энергетики»[38]. При открытии сертификата товара во вложении (RAR-архив Mask 2020.rar) находился файл Mask 2020.exe с вредоносным содержанием и шпионской программой из семейства HawkEye (aka HawkSpy).

По оценкам Сбербанка потери мировой экономики от хакерских атак в 2019 году увеличатся до $2,5 трлн. При этом ущерб России от таких атак может составить в текущем году 1,6–1,8 трлн рублей. В рамках Всемирного экономического форума в Давосе представитель Сбербанка заявил о том, что при сохранении текущего тренда к 2022 году ущерб от действий хакеров для мировой экономики может вырасти до $8–10 трлн в год[39].

Значительная часть таких атак осуществляется с целью хищения информации. Так, в первой половине 2019 г. в России более половины хакерских атак совершенны с целью хищения разноо-

[37] Киберпреступность в мире [Электронный ресурс]. URL: http://www.tadviser.ru/index.php/ (дата обращения: 29.11.2020).

[38] Троян Ginp зарабатывает на коронавирусе [Электронный ресурс]. URL: https://www.kaspersky.ru/blog/ginp-trojan-coronavirus-finder/27762/ (дата обращения: 03.04.2020).

[39] URL: https://karelinform.ru/news/society/02-10-2019/rosseti-otrazhayut-bolee-9-mln-hakerskih-atak-ezhegodno?ind=272newizv (дата обращения: 06.09.2020).

бразной информации, от личной переписки до коммерческой тайны, но особое внимание уделялось учетным данным, персональным данным и данным платежных карт. Так, например, в середине 2019 группа хакеров атаковала компьютеры представительства Европейского союза в Москве и похитила с них некоторую информацию. Кибератака продолжалась больше двух лет[40].

Начало 2020 года для России ознаменовалось беспрецедентной DDoS-атакой с которой столкнулся Сбербанк. Она была в 30 раз мощнее, чем самая мощная атака, произошедшая в 2018 году, за всю историю Сбербанка[41]. Данные показатели свидетельствуют о том, что за последние два года количество этого вида преступлений выросло в 30-раз, что свидетельствует о «хакерской эволюции»[42].

В России только за первые шесть месяцев 2020 г. российская компьютерная система, находящаяся в ведении государства, поверглась одному миллиарду хакерских атак из-за рубежа[43], более половины хакерских атак совершаются с целью хищения информации. Злоумышленники заинтересованы в самых разнообразных данных – от личной переписки до коммерческой тайны. Но по-прежнему наиболее высоко ценятся учетные данные, персональные данные и данные платежных карт.

Данные Центра мониторинга и реагирования на кибератаки Solar JSOC «Ростелеком-Солара» за «период январь–ноябрь текущего года зафиксировал более 200 профессиональных хакерских атак на российские компании, что в двое больше, чем за весь 2019 год, обращает внимание издание. При этом 30 атак совершили хакерские группировки наиболее высокого уровня»[44].

Особый вид хакерских атак отмечается в период пандемии COVID-19, преступники моментально адаптировались к сложившейся ситуации и играя на опасении и страхе за свою жизнь потер-

---

[40] BuzzFeed сообщил о похищении данных с компьютеров представительства ЕС в Москве [Электронный ресурс]. URL: https://www.interfax.ru/russia/663906 (дата обращения: 08.10.2020).

[41] Обзор: *Трубилина М.* Сбербанк столкнулся с мощнейшей DDOS-атакой [Электронный ресурс]. URL: https://rg.ru/2020/01/21/sberbank-stolknulsia-s-moshchnejshej-ddos-atakoj.html (дата обращения: 06.06.2020).

[42] *Конев Д.А.* Криминологическая безопасность и ее обеспечение в сфере цифровых технологий: постановка проблемы // Криминальная ситуация в России и антикриминальное законодательство: проблемы криминологической обусловленности закона. Москва, Российская криминологическая ассоциация. 2020.

[43] Обзор: Более миллиарда хакерских атак из-за рубежа совершено на российские госсайты с начала года [Электронный ресурс]. URL: //www: pnp.ru (дата обращения: 13.08.2020).

[44] Обзор: Эксперты выявили скачок числа кибератак на стратегические предприятия РФ [Электронный ресурс]. URL: https://www.interfax.ru/russia/739380 (дата обращения: 01.02.2021).

певших извлекали материальную выгоду. По мнению Европола, полученные результаты исследования этих преступлений позволяет выявить обновленную картину угроз и оценить дальнейшее увеличение этого вида преступности[45].

Проблему вызывают фишинговые атаки, содержащие вредоносное программное обеспечение, позволяющее преступникам используя программы, например, Ransomware, заражать файлы на устройстве путем шифрования данных и последующего отказа в доступе к ним. После блокировки компьютеров потерпевшим предлагалось заплатить за их разблокировку. Чаще всего мишенью являются объекты критической информационной инфраструктуры (банки, атомные предприятия, объекты здравоохранения, электроснабжения, военные объекты и госструктуры).

Эксперты еженедельно фиксируют появление десятков новых фишинговых ресурсов, имитирующих сайты компаний нефтяной, химической промышленности, а также предприятий сферы тяжелого машиностроения. Под удар в первую очередь попадают участники трансграничных сделок, которые ведут переписку на английском языке. Преступники включаются в переписку от имени одного из контрагентов, после чего отправляют в адрес компании фиктивные счета с измененными банковскими реквизитами и дожидаются подтверждения оплаты, в одних случаях. В других случаях, выдавая себя за представителей известных брендов, в том числе розничных сетей, строительных и нефтяных компаний, они атакуют с помощью писем с вредоносным содержанием, которые приходят по будням в рабочие часы. В данном случае их цель – заражение инфраструктуры шифровальщиком Shade/Troldesh: программа кодирует файлы на устройстве пользователя и требует у него плату за доступ к ним.

Широкое распространение получили преступные деяния с использованием банковских карт, информационно-телекоммуникационной сети «Интернет», средств мобильной связи и компьютерной техники. Более 80 % зарегистрированных преступлений в названной сфере совершены против собственности, в основном это кражи и мошенничество. Так, распространение мошенничество получило при внесении изменений в единый государственный реестр фиктивных сведений юридических лиц и индивидуальных предпринимателей, в результате которых злоумышленники полу-

[45] Поймать вирус киберпреступности, дезинформации и пандемии COVID-19» [Электронный ресурс]. URL: //https://мвд.рф/upload/site151/doc/Evropol.Doklad_Poymat_virus_kiberprestupnosti.pdf (дата обращения: 17.03.2021).

чили возможность завладеть имуществом, активами физических и юридических лиц, в том числе с государственной долей уставного капитала.

Основой этих преступлений является социальная инженерия – обман, который провоцирует пользователей на совершение последовательных действий, которые способствуют активизации вредоносного программного обеспечения. Опасность ее применения заключается в том, что от ее методов пока нет защиты.

Распространение преступности в сфере цифровых технологий и в отношении их непосредственно, «настолько велико, что еще раз подтверждает необходимость самого серьезного внимания со стороны государства к этой проблеме и взвешенного принятия решений по предупреждению правонарушений и преступлений в названной сфере»[46].

В настоящее время особую опасность представляют экстремизм и терроризм, поскольку использование новейших цифровых технологий повышает не только эффективность преступной деятельности экстремистов и террористов, позволяя обеспечить «анонимность» их финансирования, но и дает возможность объединять широкий круг разобщенных пользователей информационно-телекоммуникационных сетей, находящихся в разных точках мира. Многообразие форм их проявлений, значительное число террористических и экстремистских организаций, действующих не только в России, но и во всем мире, транснациональный характер их деятельности, увеличение количества угроз внешнего и внутреннего характера свидетельствуют о том, что деятельность по противодействию им требует особого внимания, поскольку такие явления, особенно терроризм, продолжают представлять серьезную угрозу международной безопасности[47].

---

[46] *Смольянинов Е. С.* Проблемы реализации уголовной политики по противодействию преступлениям в сфере высоких технологий / Е. С. Смольянинов, М. Ю. Воронин // Вестник РГГУ. Серия «Экономика. Управление. Право». 2018. № 3 (13). С. 134–141.

[47] *Овчинский В. С.* Иностранные боевики-террористы. Иногда они возвращаются. («Коллекция Изборского клуба»). Москва, 2019.

3.2. Криминологические риски и их влияние на состояние цифровой преступности

Нельзя не обратить внимание на объемы личной информации, размещаемой и систематизируемой в сети Интернет, которые возросли до беспрецедентных размеров. Происходящие процессы в цифровой среде способствовали появлению технологии «Больших данных» («big data»). Беспокойство вызывает развивающаяся технология больших данных, она носит универсальный характер и может использоваться во многих сферах человеческой деятельности (банковской, страховой, медицинской, правоохранительной и т. д.), организациями: предоставляющими такие данные; занимающимися их хранением; разрабатывающими алгоритмы для их анализа. Именно на основе результатов анализа этих данных будут строиться и уже строятся технологии управления. В своем послании Федеральному собранию в 2018 году Президент РФ В.В. Путин заявил о том, что «Россия должна стать одним из мировых центров хранения, обработки, передачи и защиты информационных массивов – «Больших данных»[48]. В то же время, требуется безотлагательное решение вопроса проводить деятельность по цифровому развитию страны таким образом, чтобы защитить личные данные людей и дать развиваться бизнесу. На наш взгляд, актуальным остается вопрос с принятием Закона о регулировании «Больших данных», который предоставит возможность гражданам запретить использование их личных данных операторам связи и другим компаниям; исключит факты, когда лицо на основании подписанного пользовательского соглашения предоставляет свои персональные данные для одних целей, а по факту они собираются и используются для других. В нашем понимании «Большие данные» – это прежде всего сведения в цифровом виде, колоссального объема и неоднородного содержания, которые непрерывно пополняются, обновляются и хранятся в различных источниках. Два вида больших данных: структурированные и неструктурированные

Технологии «Больших данных» носят универсальный характер и могут использоваться во многих сферах человеческой деятельности (банковской, страховой, медицинской, правоохранительной и т. д.), организациями: предоставляющими такие данные; занимающимися их хранением; разрабатывающими алгоритмы для их

[48] Послание Владимира Путина Федеральному собранию – 2018 [Электронный ресурс] // TASS.ru. 1 марта 2018 г. URL: https://tass.ru/ekonomika/4998315 (дата обращения: 15.03.2021).

анализа. Именно на основе результатов анализа этих данных будут строиться и уже строятся технологии управления, а также осуществляться менеджмент в цифровой экономике. Мы же надеемся, что эти технологии будут активно использоваться и в деятельности органов внутренних дел, поскольку такие технологии позволят исследовать преступность не только по данным статистической отчетности, но и по следам во всех источников информации. Но есть и криминологические риски использование названной технологии не только для созидания и развития общества, но и в криминальных целях, что требует подготовки соответствующей правовой основы, способствующей защите интересов юридических и физических лиц, имеющих большой оборот корпоративной, личной, семейной и т. д. информации.

Исходя из вышеизложенного, хотелось бы отметить, что «Большие данные» как правило собираются с той целью, чтобы посредством их объединения с иными базами извлечь новую информацию и применить ее, порой в преступных целях.

Особого внимания сегодня требуют развивающиеся виртуальные экономические отношения, благодаря которым активно создаются различные виды электронных платежных сервисов и технологий. Именно благодаря этим преобразованиям стали активно использоваться электронные и виртуальные деньги. В целом виртуальная валюта (криптовалюта), как разновидность виртуальной цифровой валюты, приобрела высокую популярность и в ряде стран стала не только полноценным платежным средством, но и выступает инвестиционным активом в ряде таких стран мира, как Япония, Швейцария, Швеция, Германия и др.

Существуют высокие риски как финансового, так и криминогенного свойства, связанные с виртуальной валютой (криптовалютой), поскольку отсутствует ее правовой статус, она не обеспечена ликвидными активами и какими-либо гарантиями государственного либо частного капитала, поэтому осуществление операций на «виртуальных биржах» несет высокий риск потери ее стоимости, а применение в теневой экономике позволяет обеспечить неподконтрольность национальным органам власти.

И, если в России только начинается создание правовой базы цифровых финансовых активов, куда надеемся и войдет виртуальная валюта (криптовалюта), а криминальные подходы в сфере ее оборота организованной преступностью уже отработаны.

Особое внимание сегодня требуют исследования преступлений, которые совершаются с использованием виртуальной валюты (криптовалюты). Изучение судебно-следственной практики сви-

детельствует о том, что она при совершении преступлений может выступать в качестве предмета и средства совершения преступления. При этом названная валюта может быть предметом хищения, мошенничества, вымогательства, легализации (отмывания) денежных средств. Достаточно распространенными являются случаи, когда виртуальная валюта (криптовалюта) используется в качестве средства оплаты в наркобизнесе. Увеличилось количество преступлений, связанных с легализацией (отмыванием) преступных доходов. Названные виды преступлений уже сегодня вызывают серьезную проблему, поскольку существуют технические проблемы при выявлении всех участников преступной деятельности.

Виртуальная валюта (криптовалюта) может выступать предметом составов получения (дачи) взятки и коммерческого подкупа. Довольно часто для ее добычи используется так называемый «недобросовестный» майнинг с непосредственным использованием сторонних мощностей для целей личного обогащения.

Анонимность проводимых платежей открывает широкий диапазон для «ухода от налогообложения, функционирования в теневом секторе экономики, а также повышает риски утраты валюты собственниками в случае банкротства электронных бирж по торговле криптовалютой или в результате хакерской атаки»[49]. Следует признать, что не только в экономической сфере используется виртуальная валюта (криптовалюта), она расширяет криминальные границы и в последние годы участились случаи ее использования при оплате заказных преступлений, органов и тканей человека для трансплантации, приобретенных и распространенных порнографических материалов, незаконно приобретенного оружия и боеприпасов, наркотических средств, психотропных и сильнодействующих веществ, при торговле людьми и финансировании экстремизма и терроризма, и пр.

Большую озабоченность сегодня вызывает и рост правонарушений в сфере использования искусственного интеллекта, данная технология представляет собой программно-аппаратные вычислительные комплексы полного информационного цикла (включающего восприятие, фильтрацию, обработку, хранение информации, выполнение аналитических и синтетических когнитивных функций), позволяющие в режиме человек-машина или автономно принимать

[49] *Бурыкин А. В.* Криптовалюта как виртуальный инструмент: возможности и недостатки // Перспективы формирования новой экономики XXI века. Актуальные достижения региональной науки: сборник международной научно-практической конференции, 2017.

и реализовывать решения в сложной, динамичной и неопределенной среде. Его развитие происходит в условиях увеличения анонимности. При этом соединение технологии искусственного интеллекта с сетью Интернет создают поистине безграничные возможности для преступной деятельности, что открывает большие возможности для роста преступлений в названной сфере, поскольку преступники уже в настоящее время могут без каких-либо препятствий приобрести как программные, так и аппаратные компоненты самых мощных систем искусственного интеллекта. Более того, широкое использование открытого кода в названной технологии позволяет преступникам без каких-либо затрат средств получать доступ к последним разработкам ведущих компаний. Соответственно, в будущем, по мере широкого распространения названной технологии, возрастет и количество преступлений в названной сфере, в ближайшем будущем существующие угрозы будут дополнены новыми, связанными с развитием искусственного интеллекта. Типовые угрозы станут более технически сложными и изощренными.

Искусственный интеллект «это технология тройного назначения. ИИ может быть использован как для гражданских, так и для военных целей. Отдельное направление использования ИИ – мафиозно-террористическое»[50]. При этом технология искусственного интеллекта стала активно использоваться не только в повседневной жизни, в благих целях, но и в криминальных целях. Так, известно, что такие технологии активно используются при фишинговых атаках. Большую опасность несет в себе создание комбинированных систем, включающих искусственный интеллект и роботизированные устройства. Так, например, использование дронов и иных летательных аппаратов для контрабанды наркотиков, оружия, а также использование их в целях передачи в места лишения свободы нелегально «наркотики, сигареты, мобильные телефоны, бритвенные лезвия и другую контрабанду»[51].

В некоторых случаях их используют для разведки, например, при подготовке кражи или разбойного нападения, поскольку с помощью таких дронов «изучать план собственности, где установлена какая система безопасности, где находятся хлипкие двери и окна, где расположены камеры. Все это позволяет преступникам выбрать дом или иной объект, составить детальный план и выбрать

[50] *Ларина Е.* Искусственный интеллект. Большие данные. Преступность («Коллекция Изборского клуба»). Москва, 2018.

[51] *Плеханов И.* Военные новости: разведывательные дроны преступников [Электронный ресурс]. URL: https://inosmi.ru/social/20180508/242170511.html (дата обращения: 19.02.2021).

маршрут для взлома. С помощью дронов можно также установить график пребывания хозяев или охраны на объекте, привычки владельцев, количество людей и так далее»[52].

В ближайшем будущем существующие угрозы будут дополнены новыми, связанными с развитием искусственного интеллекта. Типовые угрозы станут более технически сложными и изощренными.

Особое внимание уделяется сегодня не только развитию технологии Интернета вещей, и преступной деятельности в сфере названной технологии. Технология Интернет вещей представляет собой сеть физических предметов («вещей»), подключенных к Интернету и взаимодействующих между собой или с внешней средой. При этом следует отметить, что данная технология уже активно используется. При этом эксперты прогнозируют, что в ближайшие годы самым быстрорастущим сегментом интернета вещей станут устройства «умного дома», включая бытовые электроприборы и датчики систем вентиляции, отопления, видеонаблюдения. Интернет вещей продолжает выстраивать глобальную информационную сеть длиною в целое поколение. Здесь можно выделить два пересекающихся направления: создание «умных» подключенных продуктов и сбор данных для улучшения результатов бизнес-деятельности. Различные секторы и компании сосредоточивают свои усилия на том или ином направлении. К первому направлению относятся известные потребительские устройства – от «умных» часов и терморегуляторов до роботизированных помощников по дому и даже подключенных автомобилей. Второе направление включает промышленный Интернет вещей, с помощью которого производители и другие участники рынка осуществляют сбор данных с оборудования и других источников и их последующий анализ в целях оптимизации своих процессов, прогнозирования и предотвращения проблем и, в конечном итоге, создания более совершенных экосистем для новых продуктов и услуг, а также сбора и обработки данных, в том числе и в промышленных целях.

Нельзя обойти стороной и вопросы, которые волнуют сотрудников правоохранительных органов – это преступления в сфере интернета вещей, поскольку здесь проявляется особый интерес криминальных сообществ. Это обусловлено, во-первых, серьезными последствиями, поскольку еще не подготовлены технологии, которые бы способствовали снижению уровня рисков при использовании таких комплексов повсеместно и повышением уровня криминологических рисков, связанных с посягательствами на них.

[52] *Там же.*

По некоторым оценкам, количество посягательств на устройства интернета вещей постоянно увеличивается. Так, в 2018 г. по сравнению с предыдущим выросло на 217,5 %. В первой половине 2019 года специалисты компании «Лаборатория Касперского» «зафиксировали 105 млн атак на IoT-устройства, исходящих с 276 тыс. уникальных IP-адресов. Данный показатель в семь раз больше, чем в первой половине 2018 года, когда было обнаружено около 12 млн атак с 69 тыс. IP-адресов. Пользуясь слабой защитой IoT-продуктов, киберпреступники прикладывают больше усилий для создания и монетизации IoT-ботнетов»[53]. Под стать растут и расходы на обеспечение безопасности интернета вещей: по прогнозам Gartner, расходы компаний на обеспечение их защиты в 2017 г. достигли $1,17 млрд, а к 2021 г. сумма превысит $3 млрд. Нельзя также исключать корректировок этих цифр в сторону значительного увеличения в последующие годы.

По мнению экспертов, Интернет вещей (англ. Internet of Things, IoT) в совокупности с искусственным интеллектом, большими данными и блокчейн технологией составляет суть новой промышленной революции[54]. Особое внимание уделяется сегодня и преступной деятельности в сфере интернета вещей, поскольку, с одной стороны, развитие этой технологии может повысить эффективность, поднять производительность, снизить количество отходов, подстегнуть экономический рост. С другой же стороны, криминологические риски атак со стороны преступников, террористов и иных злоумышленников увеличиваются.

Проводя итог следует отметить, что пока не выработаны достаточные эффективные механизмы выявления и пресечения преступлений, совершенных в сфере цифровых технологий и сложно квалифицировать, и выявлять субъектов преступлений, в том числе и субъектов хакерских атак. Настало время изменить стратегию и тактику противодействия преступлениям, совершаемым в сфере цифровых технологий. Необходимо изучение и определение криминологических угроз и рисков, которые позволят определить прогноз о том, «как будет меняться структура преступности, какие будут появляться новые формы организации преступных сообществ, как изменяется преступное поведение под воздействием технологий

[53] Информационная безопасность интернета вещей (Internet of Things) [Электронный ресурс]. URL: https://www.tadviser.ru/index.php/Статья:Информационная_безопасность_интернета_вещей_(Internet_of_Things) (дата обращения: 10.03.2021).

[54] *Ларина Е.* Криминальный шлейф интернета вещей [Электронный ресурс] / Е. Ларина, В.С. Овчинский. URL: http://hrazvedka.ru/blog/kriminalnyj-shlejf-interneta-veshhej.html (дата обращения: 04.02.2021).

новой технологической революции и т. п.». Более того, основой такой работы должны стать результаты работы с использованием методов и программ искусственного интеллекта и анализа больших данных. Такая подготовка должна вестись совершенно на новом уровне.

Необходимо нормативное регулирование цифровых технологий и разработка уголовно-правового механизма противодействия преступлениям, совершаемым с их использованием, но самое главное – это подготовка специалистов, которые способны будут противостоять всем криминологическим рискам и угрозам.

Контрольные вопросы

1. Определите основные криминологические риски цифровых технологий.
2. Проанализируйте современное состояние цифровой преступности.
3. Рассмотрите особенности преступлений, совершаемых с использованием искусственного интеллекта.
4. Какова взаимосвязь цифровой преступности с организованной преступностью, терроризмом и экстремизмом и т. д.?

Глава 4. Причинный комплекс цифровой преступности

Планируемые результаты освоения темы главы

– **знать** понятие причинного комплекса цифровой преступности, причины и условия, способствующие совершению цифровых преступлений;

– **уметь** своевременно определять основные направления исследования причин и условий, способствующих совершению цифровых преступлений для эффективной работы по противодействию названному виду преступности;

– **владеть** навыками анализа информации о причинном комплексе цифровой преступности, оценки криминологической ситуации, сколадывающейся в тот или иной период времени, влиянии на нее причин и условий, способствующих совершению цифровых преступлений и применять полученные знания на практике.

4.1. Общая теория причинности и цифровая преступность

Предупредительная деятельность невозможна без исследования причинного комплекса цифровой преступности, поскольку ее результаты должны быть положены в основу подготовки мер по противодействию преступности и повышению эффективности предупреждения деятельности правоохранительных органов.

Характеризуя причинность, следует рассматривать ее как объективную, генетическую (производящую порождающую) связь. Она рассматривается как одна из форм универсального взаимодействия между причиной и следствием[55]. В связи с этим следует согласиться с мнением А. И. Долговой, которая утверждает, что «причина, производя действие порождает следствие, она всегда предшествует следствию, а следствие, в свою очередь, не может быть причиной и она (причина) не может быть сведена к следствию»[56]. Но нельзя забывать, что взаимосвязь «причина-следствие» возможна только при совокупности необходимых условий, поскольку в механизме причинности преступности причина порождает следствие, а усло-

[55] Материалистическая диалектика. Москва, 1982. Т. 1. С. 210–228.

[56] В криминологической доктрине используются такие категории, как «причина и следствие», «причинно-следственные связи», «причинные комплексы», и др. (см. Криминология: учебник для вузов / под ред. А. И. Долговой. Москва, 2001).

вие способствует этому. Такого же мнения придерживается и ряд авторов[57].

В тоже время, несмотря на общепринятое мнение в криминологической доктрине о разделении социальных явлений и процессов, детерминирующих преступность, на причины и условия, в правоприменительной практике, разграничить их очень сложно. Это обосновано тем, что они, причины и условия, могут меняться местами, заменять друг друга. Более того, условия сами не могут породить преступление, но без их наличия причина не может ни сформироваться, ни реализоваться. Поэтому на вопрос о том, что же относится к причинам преступности, а что к условиям ее существования, криминологи отвечают неоднозначно[58].

Причинное объяснение этого явления – необходимое составляющее любого криминологического исследования, способное указать на то, какие процессы порождают данное явление, в каких конкретных условиях оно может возникнуть.

На теоретическом уровне существует множество подходов к определению причин и условий преступности в целом[59]. Так, причины противоправного поведения называют по-разному: факторы, криминогенные детерминанты, обстоятельства преступлений, условия. На наш взгляд, все эти термины, так или иначе, обозначают однопорядковые явления[60], поэтому совершенно справедливо, указывая на сложность разграничения причин и условий преступности, возможности их трансформации из одного качества в другое[61]. Ряд криминологов использует термин факторы, обозначающий как причины, так и условия.

В научных работах особо подчеркивается, что причины и условия преступности социальны по своему происхождению и сущности. Так, например, по мнению Н. Ф. Кузнецовой: «Причины и условия преступности – это система негативных для соответствующей общественно-экономической формации и данного государства

---

[57] Криминология: учебник / под ред. проф. Н.Ф. Кузнецовой, В.В. Лунеевой. Москва, 2004. С. 166–167; *Старков О.В.* Криминология: Общая, Особенная и Специальная части: учебник. Санкт-Петербург, 2012. С. 132–134.

[58] См.: *Кудрявцев В.Н.* Причины правонарушений. Москва, Наука. 1976; *Кузнецова Н.Ф.* Проблемы криминологической детерминации. Москва, МГУ. 1984; *Яковлев А.М.* Теория криминологии и социальная практика. Москва: Наука. 1985.

[59] *Там же.*

[60] См.: Криминология. М., 1979; Криминология. Москва, 1988. С. 115; Криминология и профилактика преступлений. Москва, 1992.

[61] См.: *Мошак Г.Г.* Указ. соч. С. 83; *Коробейников Б. В., Селиванов Н. А., Скворцов К.Ф.* Изучение факторов, влияющих на изменение уровня и структуры преступности // Советское государство и право. 1982. № 1.

социальных явлений, детерминирующих преступность как свое следствие»[62].

Такая позиция является господствующей в системе современной криминологии. Отдельные попытки переоценить роль биологических факторов в системе причин преступности не получили широкого распространения, поскольку считается общепризнанным, что ни одно социальное явление не может быть объяснено с помощью биологических теорий.[63] Вместе с тем современные криминологи не отрицают, что биологические особенности личности хотя и не порождают преступности, но оказывают значительное влияние на поведение человека, являются базой для восприятия человеком социальной программы[64].

Учитывая тот факт, что причин и условий, совместные действия которых вызывают следствие, большое количество, мы будем говорить о причинном комплексе цифровой преступности как о «совокупности факторов и связанных с ними социальных противоречий, детерминирующих криминогенность»[65]. Исследование причинного комплекса криминогенности цифровой преступности позволит раскрыть природу этого явления, объяснить ее происхождение, показать особенности, способствующие сохранению ее высокого уровня. Так, например, только в 2020 г. в связи с таким социальным явлением как пандемия COVID-19 изменился и усугубился причинный комплекс и увеличились криминологические риски. Это подтверждается и мнением председателя Счетной палаты А. Кудрина, который считает «за последние пять лет уровень жизни в нашей стране снизился практически на десять процентов. Данный показатель во втором квартале 2020 года достиг 8 %, а в третьем зафиксирован спад – 4,5 %»[66], это свидетельствует о том, что «количество бедных в России вырастет примерно на один миллион человек. В ближайшие годы ситуация кардинальным образом не изменится»[67]. Более того, он также отметил, что в ближайшее время неизбежно возник-

---

[62] Криминология. Москва, Изд-во МГУ. 1994.

[63] См.: *Ной И.С.* Методологические проблемы советской криминологии. Саратов, 1975.

[64] См.: *Дубинин Н. Д., Карпец И. И., Кудрявцев В.Н.* Генетика, поведение, ответственность. 2-е изд., перераб. и допол. Москва, 1989; *Кудрявцев В.Н.* Социальные деформации. М., 1992.

[65] *Клюковская И.Н.* Современное состояние коррупции в России и проблемы ее предупреждения. Ставрополь, 2001.

[66] URL: https://www.rbc.ru/finances/13/04/2020/5e942e2b9a794789aaf7034e (дата обращения: 13.01.2021).

[67] *Там же.*

нут проблемы у банков, поскольку пострадавшие от пандемии юридические и физические лица не смогут оплачивать ранее полученные кредиты. В целом в перспективе будет расширяться преступная деятельность, меняясь не только количественно, но и качественно, а учитывая тенденции цифровой преступности, то, при наличии особенностей причинного комплекса, она будет только увеличиваться. Представленные данные свидетельствуют о том, на сколько серьезные изменения, происходящие в обществе, влияют на криминологические риски и причинный комплекс преступности.

Известно, что в ходе изучения причинного комплекса цифровой преступности следует обращать внимание на комплексные блоки причин и условий, способствующих совершению преступлений. К ним следует отнести социально-политические, социально-экономические, социально-правовые, организационно-технический и иные. При характеристике этой группы преступлений, как представляется, следует остановиться на анализе трех блоков, это социально-экономический, правовой и организационно-технический.

4.2. Основные причины и условия цифровой преступности

Исследуя причинный комплекс цифровой преступности и учитывая тот факт, что более подробно он будет рассмотрен при характеристике отдельных видов преступности, позволим себе рассмотреть в этом параграфе только основные блоки, присущие всем видам цифровой преступности. К ним следует отнести социально-экономические, социально-политические, социально-психологические, воспитательные, правовые и организационно-управленческие причины.

Анализ особенностей социально-экономических причин и условий, способствующих совершению преступлений в сфере цифровых технологий конечно же лежит в основе экономических отношений, вызванных длительными кризисными явлениями в современной России, нестабильностью экономической политики, которые влияют на социальную и экономическую не стабильность, а в последние годы в России все чаще обращают нас себя внимание, выступили своеобразным «стимулятором роста криминогенности».

Нельзя забывать и о том, что с утверждением программы «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы»[68], согласно которой «стратегически важным вопросом для России в целом, определяющим ее конкурентоспособность на мировой арене является развитие цифровой экономики»[69] и принятии программы «Цифровая экономика Российской Федерации»[70] стали стремительно развиваться технологии цифровой экономики, потенциал которых сегодня, во-первых, распространяется во все сферы деятельности современного общества, стремительно вытесняя старый уклад, старое мышление и устаревшие технологии. Во-вторых, цифровая экономика и развитие цифровых технологий несет в себе огромный потенциал криминологических рисков, о чем свидетельствуют результаты проведенных исследований, поскольку правовая основа, организационно-управ-

---

[68] О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: указ Президента Российской Федерации от 9 мая 2017 г. № 203. Доступ из информационно-правового портала «Гарант».

[69] *Пинкевич Т.В.* Развитие цифровой экономики и ее влияние на криминологическую безопасность России // Уголовная политика и правоприменительная практика: сборник статей по материалам V Всероссийской научно-практической конференции 3 ноября 2018 г. / под ред. д-ра юрид наук, доцента Е.Н. Рахмановой. Северо-Западный филиал ФГБОУВО РГУП, Санкт-Петербург, 2019.

[70] Об утверждении программы «Цифровая экономика РФ»: распоряжение Правительства Российской Федерации от 28 июля 2017 г. № 1632-р. Доступ из справ.-правовой системы «КонсультантПлюс».

ленческие составляющие антикриминальные инструменты еще находятся на стадии разработки, а представители организованных преступных формирований уже используют новые технологии в преступных целях[71].

И поскольку не разработаны механизмы защиты цифровых технологий, методологические подходы к ее оценке, ее реализации в условиях цифровой экономики и контроля над этими процессами, это существенным образом влияет на характер и результаты использования цифровых технологий и на рост преступности.

Так, внедрение цифровых технологий приведет к резкому росту безработицы. Это связано с тем, что внедрение, например, технологии распределительного реестра, искусственного интеллекта, робототехники способствует сокращению рабочих мест. Из-за новых технологий в мире исчезнут миллионы рабочих мест. Так, например, глава Сбербанка Г. Греф заявил о том, что в ближайшее время в названной организации будет работать в лучшем случае тысяча. Одни эксперты прогнозируют, что «через 10 лет треть профессий отомрет. Уйдет часть экономистов и юристов, за которых начнут работать роботы... Цифровизация и переход на другие модели управления, профилактику любых нарушений существенно сократят потребность в чиновниках, и решения будут приниматься автоматически... будет не хватать 1 млн программистов, которые будут заниматься оцифровкой в любой отрасли»[72]. Другие эксперты считают, что «для прорыва нам не нужен миллион программистов, нам нужно, по нашим подсчетам, 120 тысяч высококвалифицированных инженеров и программистов, потому что, если мы переучим всех, и они будут не очень грамотные»[73].

Прогноз экспертов свидетельствует о том, что ближайшие годы будут отмечены кардинальными изменениями на рынках труда, изменениями профессий, требующих от работника новых навыков. Сократится количество программ средних специальных учебных заведений (колледжей), обучающих ряду профессий, которые через 3–4 года будут не востребованы. Так, в 2019 г. в России из учебных программ исчезли почти сто профессий, которым обучались ранее

[71] *Пинкевич Т.В.* Проблемы противодействия организованной преступности в сфере цифровой экономики // Борьба с организованными проявлениями преступности и обеспечение национальной безопасности Российской Федерации // под ред. д-ра юрид. наук, профессора А.И. Долговой. Москва, Российская криминологическая ассоциация, 2019.

[72] Кудрин: часть экономистов и налоговиков через 10 лет могут заменить роботы [Электронный ресурс]. URL: https://tass.ru/ekonomika/4717521 (дата обращения: 18.03.2021).

[73] URL: Bibliodose_k_PS_20.02.18_d1(2)_d1(2).docx (дата обращения: 20.01.2021).

выпускники школ. Если не предвосхищать и не решать такие вопросы своевременно в ближайшие годы может обернуться огромными экономическими и социальными издержками. Все это ставит вопрос о комплексной стратегии подготовки кадров с новыми навыками, соответствующими современным стратегиям развития и трендам современной технологической революции.

Согласно анализу компаний Microsoft и The Future Laboratory, 65 % нынешних школьников и студентов займут должности, которых еще не существует. По прогнозу специалистов к 2025 году наиболее востребованными станут дизайнеры виртуальной среды обитания, адвокаты по робоэтике, биохакеры на фрилансе. При этом специалисты будущего будут владеть несколькими навыками.

Высокий уровень безработицы всегда отрицательно влияет на криминогенную ситуацию, поскольку криминальный потенциал определенного слоя безработных ориентирован на включение в криминальный бизнес организованной преступности. Безработица, как отмечает В. Е. Эминов, является «резервом преступности, что, по его мнению, «доказано всей историей развития человечества»[74]. Существовала убежденность в том, что новые отрасли вберут в себя оставшихся без работы людей. К сожалению, реальность оказывается иной. Число людей, занятых в технологическом секторе, остается скромным, около 5–6 % всей рабочей силы. А чем будут заниматься сегодняшние несовершеннолетние, через 10 лет, а их в стране 27 374 000, из них 26 % (7 110 220 чел.) проживают в малоимущих семьях и в силу сложившихся обстоятельств не смогут получить соответствующего образования.

Негативное влияние на криминогенную ситуацию оказывает снижение уровня жизни значительной части граждан. По сведениям исследования экспертов OMI и «Платформы»[75] более 50 % работающих россиян сообщили о значительном падении дохода семьи с начала распространения коронавируса. Названные явления приведут к рост миграции, особенно будет нарастать ее внутренняя часть, население будет мигрировать внутри страны с целью найти заработок, получить возможность жить в благоустроенном жилье и т. д. Принято считать, что такие явления, как миграция и теневая экономика тесно взаимосвязаны.

---

[74] *Эминов В. Е.* Причины преступности в России: криминологический и социально-психологический анализ. Москва, 2011.

[75] Росстат отчитался о сокращении реальных располагаемых доходов россиян. Основной удар по доходам населения из-за коронавируса придется на второй квартал [Электронный ресурс]. URL: https://www.rbc.ru/economics/26/04/2020/5ea40aaf9a7947217fbda5f9?from=materials_on_subject (дата обращения: 09.12.2020).

Следует также обратить внимание и на проблему социального и цифрового неравенства. В теории криминологии с момента ее возникновения в XIX в. неравенство относили к числу главных причин преступности. С начала XXI в. во всем мире слово «неравенство» не сходит со страниц газет и экранов телевизоров. Большинство исследователей полагают, что экономическое неравенство – это главное зло, с которым сталкивается современное общество. Мы уже сегодня сталкиваемся с проблемой цифрового неравенства, информационного неравенства, когда представители социальной группы зачастую ограничены в возможности иметь доступ к современным средствам коммуникации. Цифровой барьер является термином социально-политического характера. На возможности ущемленной группы влияют отсутствие или ограниченный доступа телевидению, Интернету, телефонной связи (мобильной и стационарной), радио. Все это ограничивает возможности этой группы в поиске работы, налаживании социальных связей, культурном обмене и может негативно влиять на экономическую эффективность, развитие и сохранение культуры, уровень образования.

Согласно общепринятым воззрениям на цифровое (информационное) общество, его специфика такова, что свободный обмен информацией способствует преодолению нищеты и неравенства, однако у тех, кто отключен от такого обмена, перспективы катастрофически ухудшаются.

В данном случае не так важно, какими конкретно причинами продиктовано наличие цифрового неравенства между теми, кто может пользоваться благами и соблазнами Сети, и остальным миром. Существенно другое: цифровое будущее провоцирует возникновение «новых бедных». В эту группу можно зачислять не только тех, кто по объективным причинам лишен возможности доступа к Интернету и цифровым устройствам. Сюда же попадают и пользователи, некачественно применяющие предложенные технические возможности. Кажется, что разница между этими группами велика, но это не совсем так. Первые не могут познакомиться с плодами научно-технической революции, вторые – осознанно или нет – не хотят. Результат в обоих случаях плачевный – будущее наступает без них.

При усилении социального расслоения рост преступности очевиден. Развитый мир во многом от массовой «уличной» преступности отвык за последние пару десятков лет. Это следствие и роста уровня жизни, и компьютеризации: компьютерные игры значительную часть агрессии загнали в виртуальный мир. Конечно, бывают

и «выбросы» этой агрессии в мир реальный, но все же это не массовое явление.

В связи с возможной массовой безработицей и неизбежным крушением социальных государств в том виде, в каком они возникли во второй половине XX в., новый всплеск преступности станет реальной опасностью.

В условиях неоднозначных перспектив экономического развития будет все сложнее удовлетворить общественные запросы и обеспечить криминологическую безопасность. Эти усилия будут сдерживаться фискальными ограничениями, растущей политической поляризацией, увеличивающимся разрывом между динамикой технологий, законами и нормами, лежащими в основе государственной власти.

Социально-политические причины распространения преступлений в сфере цифровых технологий взаимосвязаны социально-экономическими причинами поскольку политическая нестабильность всегда обостряет экономическую и социальную ситуации. Поэтому «политика, политическая ситуация в стране, которая влияет на весь комплекс отношений в обществе определяет государственную стабильность. Если же политическая власть нестабильна, то регулирование общественных отношений меняется в отрицательную сторону и влечет снижение жизненного уровня населения, их незащищенность в правовой и социальной сферах. И как следствие – наступают негативные последствия, а именно – рост преступности»[76].

Исследование причинного комплекса цифровой преступности свидетельствует о том, что важную роль здесь играют причины социально-правового характера. Развитие цифровых технологий сегодня находится в стадии становления. Однако их развитие сопряжено и с созданием нормативной базы и не только для использования цифровых технологий, но и для защиты в целом личности, общества и государства. Необходима подготовка административных регламентов для специалистов, работающих с цифровыми технологиями и применяющими их во всех сферах жизнедеятельности общества. Это, прежде всего, такие сферы применения, как цифровое управление, цифровая логистика, цифровая медицина, электронная коммерция, умный дом и умный город, и пр. Их применение с одной стороны работает во благо, улучшая жизнь граждан, с другой несет

[76] *Мандрыко А.В.* Уголовно-правовые и криминологические меры противодействия преступности в сфере интеллектуальной собственности: дис. ... канд. юрид. наук. Москва, 2017.

в себе огромный потенциал криминологических рисков, о чем свидетельствуют результаты проведенных исследований, поскольку правовая основа, организационно-управленческие составляющие антикриминальные инструменты еще находятся на стадии разработки, а представители организованных преступных формирований уже используют новые технологии в преступных целях[77].

Создание в России соответствующей правовой базы продолжается, часть концептуальных вопросов решена с принятием ряда общих нормативных актов, что же касается частностей, то здесь еще остается много проблем. В настоящее время существуют единичные нормативно-правовые акты, регулирующие отдельные направления в развитии цифровых технологий и ряд сложных проблем в данной сфере остается нерешенным. Так, например, отсутствие административных регламентов по применению искусственного интеллекта, даже слабого, который активно используется в настоящее время, может быть опасен для людей. Это непременно будет влиять и на уровне криминогенности в обществе и снизит экономическую эффективность из-за несовместимости отдельных составляющих робототехнических комплексов с искусственным интеллектом и контролем человека.

Требует особого внимания и законодательное регулирование искусственного интеллекта и робототехники, в части определения субъекта, использующего автоматизированные транспортные средства и беспилотные летательные аппараты, поскольку в случае ошибки указанных аппаратов сложно определить виновного и понять, почему искусственный интеллект принял то или иное решение в определенной ситуации. Принятая Национальная стратегия развития искусственного интеллекта на период до 2030 года определила «цели и основные задачи развития искусственного интеллекта в Российской Федерации, а также меры, направленные на его использование в целях обеспечения национальных интересов и реализации стратегических национальных приоритетов, в том числе в области научно-технологического развития»[78]. Однако необходима подготовка и принятие концепции регулирования искусственного интеллекта или конвенции о робототехнике и искус-

[77] *Пинкевич Т. В.* Проблемы противодействия организованной преступности в сфере цифровой экономики // Борьба с организованными проявлениями преступности и обеспечение национальной безопасности Российской Федерации / под ред. д-ра юрид. наук, профессора А. И. Долговой. Москва: Российская криминологическая ассоциация, 2019.

[78] Национальная стратегия развития искусственного интеллекта на период до 2030 года: указ Президента Российской Федерации от 10 октября 2019 г. № 490. Доступ из справ.-правовой системы «КонсультантПлюс».

ственном интеллекте, в которых будут сформулированы правила робототехники, изложены проблемы и возможные пути их решения, с которыми может столкнуться общество, развивая искусственный интеллект.

Несмотря на то что в текущем году внесены изменения в Федеральный закон «О персональных данных» в части использования большие данных и подготовлен законопроект, предусматривающий нововведения в Закон об информации (требования об обязательном информировании пользователя об обработке связанных с ним больших данных), необходима подготовка и принятие самостоятельного Закона о больших данных, с целью ограничения использования личных данных третьими лицами в преступных целях. Аналогично обстоит вопрос с нейротехнологиями, которые ставят свободу разума под угрозу, то требует подготовки и принятия законодательных актов, направленных на защиту умственной свободы, психической неприкосновенности и психологической преемственности.

Не определено на законодательном уровне правовое положение использования: квантовых компьютеров, которые смогут предугадывать «шаги» хакеров в миллионах или миллиардах возможных итерациях. Квантовая мощь позволит осуществлять квантовое шифрование, но в то же время хакеры беспроблемно смогут взламывать самые сложные методы безопасности, которые обеспечиваются относительно примитивными машинами 20; новых производственных технологий, к примеру установок аддитивного производства (3D-печати). С помощью 3D-принтеров возможно распечатать предметы для совершения преступлений: оружие, ключи, подделки произведений искусства и сканеры, способные дублировать практически любые запатентованные трехмерные предметы и многое другое. Государственная Дума Российской Федерации в этом направлении только предлагает ввести обязательную регистрацию 3D-принтеров.

Безопасность интернета вещей складывается из безопасности связи, защиты и контроля устройства, контроля взаимодействий в сети. Так злоумышленники, используя уязвимости данных технологий, могут подслушивать конфиденциальные разговоры, а затем использовать их в преступных целях. В Законах об информации и связи говорится о безопасности беспроводной передачи данных, где при авторизации, пользователь в обязательном порядке должен пройти идентификацию личности и своего гаджета. Идентификация необходима при общественном доступе к wi-fi в общественных местах (кафе, библиотеках, школах, парках и т. п.). Однако ничем не регулируется использование точек доступа, установленных част-

ными лицами, к которым пользователи могут подключаться анонимно, в том числе используя их в противозаконных целях.

Виртуальная и дополненная реальность также представляют определенную угрозу для общества. Очень часто в средствах массовой информации мы слышим о совершении подростками преступлений под влиянием компьютерных игр. Погружение ребенка в виртуальную (дополненную) реальность в игре помимо физических воздействий на организм виртуального путешественника может оказывать и психическое воздействий, в том числе на восприятие пользователем самого себя.

Относительно системы распределенного реестра или блокчейна, следует отметить, что разработана и принята дорожная карта его развития. Дорожная карта допускает применение блокчейна в финансовой деятельности, промышленности, транспортировке и госуправлении, предлагается его использование во всех государственных информационных системах, в том числе при голосовании на муниципальном уровне и при контроле за расходованием бюджетных средств[79]. Однако механизм обеспечения криминологической безопасности в этой сфере в дорожной карте не прописан.

К организационно-техническим причинам цифровой преступности можно отнести определение основных направлений профилактической работы, обеспечение взаимодействия с иными субъектами профилактики; техническая оснащенность правоохранительных органов новейшими технологиями цифрового мира; осуществление криминологической пропаганды и обучения граждан правовым основам цифрового права.

Нельзя забывать, что преступность цифровых технологий детерминирует и другие социально-правовые явления, которые следует учитывать при характеристике причинного комплекса цифровой преступности. К их числу относятся явления, процессы, факторы, которые порождают, оживляют, укрепляют и поддерживают в общественном сознании антисоциальные взгляды, тенденции, привычки, лежащие в основе антиобщественного поведения, либо непосредственно вызывают или облегчают совершение преступлений.

Немалую роль в причинном комплексе играет нравственно-психологический кризис.

---

[79] Триллион проведут по цепи. «Ростех» представил «дорожную карту» развития блокчейна в России [Электронный ресурс]. URL: https://www.kommersant.ru/doc/3977352 (дата обращения: 11.04.2021).

Все рассмотренные криминогенные детерминанты не являются чем-то изолированным, они, в действительности, переплетаются, создавая общий неблагоприятный фон для совершения цифровых преступлений.

Контрольные вопросы

1. Определите основные причины и условия цифровой преступности.
2. Проанализируйте социально-экономические причины цифровой преступности.
3. Рассмотрите особенности социально-политических причин и условий, способствующих совершению цифровых преступлений.
4. Какова взаимосвязь развития цифровых технологий и роста цифровой преступности?

Глава 5. Личность преступника, совершившего преступление в сфере цифровых технологий

Планируемые результаты освоения темы главы

– **знать** понятие личности совершившего преступление в сфере цифровых технологий, ее основные характеристики и типы;

– **уметь** типологизировать личность совершившего преступление в сфере цифровых технологий, определять основные ее свойства; применять полученые знания в практической деятельности;

– **владеть** терминологией категории «личность преступника»; навыками для организации и проведения криминологических исследований личности преступника; составления индивидульно-профилактических программ.

5.1. Значение изучения категории «личность преступника» в органах внутренних дел

Категория «личность преступника» относится к центральному объекту криминологического анализа. Задача изучения этой криминологической категории состоит в выявлении и анализе личностных качеств, свойств и черт, продуцирующих преступное поведение и определяющих пути дальнейшей его профилактики. «Личность преступника» можно представить, как «совокупность свойств, присущих, совершающему или совершившему преступление, человеку, составляющих его индивидуальность».

Проблемы личности преступника являются ключевыми не только в теоретическом аспекте для криминологии, но и в практическом для осуществления работы по предупреждению преступности органами внутренних дел, в число которых входят оперативные подразделения. Предупредительная деятельность органов внутренних дел основывается на знаниях криминологической науки, изучающей закономерности и тенденции развития преступности, ее причины и условия, личность преступников, механизм детерминации и генезис преступного поведения. Личность преступника в процессе принятия решения, подготовки и совершения преступлении проявляет себя в динамике, взаимодействует с внешними и внутренними факторами окружающей действительности в результате чего можно вычленить криминологически значимую информацию,

которая отображает личностные особенности, планирующего либо совершившего преступление лица.

Концепцию «личности преступника», как объекта профилактики преступлений следует рассматривать в рамках криминологической системы выверенных взаимосвязанных принципов, идей, знаний и гипотез, используемой в деятельности органов внутренних дел с целью описания, выявления особенностей граждан, которые с большей степенью вероятности могут совершить, совершают или совершили преступление. Эта концепция объясняет прошлые и настоящие характеристики обозначенной личности (причем в прошлом – законопослушной, не совершившей или готовящей совершение преступление), а также прогнозирует ее будущее состояние.

Основная цель этой концепции – раскрытие законов субъективных реалий, состояний, процессов, свойств внешнего и внутреннего мира, как эти свойства накладываются на личность и проявляются в конкретных условиях. Она объясняет источники существующих противоречий, процессов качественных негативных изменений во внутреннем развитии личности, рассматривает внутренние процессы личности преступника в их сложной динамике.

Концепция «личности преступника» обладает прогностической важностью, давая органам внутренних дел возможность прогнозировать индивидуальное преступное поведение, разрабатывать методику такого прогнозирования. Без прогностической составляющей невозможно эффективно реализовывать стоящие перед различными подразделениями органов внутренних дел задачи, особенно тех, чья работа строится на анализе индивидуальной характеристики, оперативной обстановки и прогнозе вероятностного развития преступного поведения или события.

Достаточно давно было констатировано, что теоретическое изучение личности в криминологической науке является основой для практических рекомендаций, применяемых при осуществлении индивидуальной профилактики преступлений, осуществляемой органами внутренних дел[80].

Личность преступника в криминологии – это понятие, выражающее социальную сущность преступников разных типов, сложный комплекс характеризующих их признаков, свойств, связей, отношений, их нравственный и духовный мир, взятые в развитии, во взаимодействии с социальными и индивидуальными жизненными усло-

[80] *Антонян Ю.М.* Основные черты теории личности преступника в криминологии // Советское государство и право. Москва, 1984. № 3.

виями и в той или иной мере определяющие совершение преступлений. Познать личность преступника возможно путем изучения ее структуры, которая представляет собой многообразие личностных качеств, объединенных в определенные группы[81], для органов внутренних дел определяющее значение имеют именно обобщенные, типологические данные о личности преступников (включая и цифровых преступников), о процессе формирования определенных свойств, которыми характеризуется преступник.

Базисной причиной совершения противоправного деяния является деформация определенных субъективных качеств лица, а именно – ценностно-морального ряда. Определенные ситуации и окружающая социальная среда запускают механизм существующих противоречий в человеке, его психологических особенностей. Внешние условия, накладываясь на специфические черты личности, которые предрасполагают к негативному поведению, приводят к совершению цифрового противоправного деяния.

Причины индивидуального преступного поведения можно увидеть и во внутренних свойствах личности. В основе совершения личностью как социально-положительных, нейтральных, так и социально-опасных действий, по мнению А. Р. Ратинова, лежат ценностные ориентации[82]. О том, что деформированная мораль и правосознание сами по себе могут стать причиной выбора преступного поведения, писали А. Р. Ратинов и И. И. Карпец[83]. А. И. Долгова связывала криминальное поведение с такими личностными признаками, как потребности, моральные свойства, ценностные ориентации и правосознание[84].

Существенное значение имеют знания криминологии о мотивации преступного поведения (криминальной мотивации), так как они помогают «думать» за преступника, что является важнейшим интеллектуальным началом оперативно-разыскной тактики. Имеется в виду реконструкция возможных действий преступников (прошлых и предстоящих) с учетом их преступной квалификации и преступного опыта. Когда сотрудник ОВД знает, что предполагал, как поступал преступник и почему именно так, а не иначе, – он может

---

[81] *Ищук Я. Г.* Характеристика личности условно осужденного, совершившего преступление // Уголовно-исполнительное право. Рязань, 2011.

[82] *Ратинов А. Р.* Психология личности преступника. Ценностно-нормативный подход // Личность преступника как объект психологического воздействия. Москва, 1979.

[83] *Карпец И. И., Ратинов А. Р.* Правосознание как элемент правовой культуры // Правовая культура и вопросы правового воспитания. Москва, 1974.

[84] Курс советской криминологии. Предмет. Методология. Преступность и ее причины. Преступник. Москва, 1985.

достаточно ярко представить себе (смоделировать) не только его социальный, нравственный облик (отнести его к соответствующему социальному типу личности), но и его индивидуальный образ. А это имеет большое значение для ориентирования сил и средств ОВД на выявление преступника и предотвращения преступления.

Так, иерархия мотивов современных преступников, которые совершают преступления в сфере цифровых технологий цифровых выглядит следующим образом: в 65 % случаях у преступников присутствовал корыстный мотив, при этом 8 % интернет-преступников удовлетворены своим доходом, 69 % не удовлетворены и 23 % нуждаются; у 12 % были хулиганские побуждения; 11 % совершили преступление из любопытства (исследовательский интерес); 6 % при совершении деяния из-за влияния извне (например, совершение интернет-преступлений в составе преступных групп); 4 % из политических мотивов; 2 % из чувства мести.

В трудах Г.С. Саркисова прямо указывается на объект индивидуальной профилактики преступлений. «Можно утверждать, – пишет он, – что объектами индивидуально-профилактического воздействия являются искажения (деформации, рассогласования) ценностно-нормативной системы индивида, поддерживаемые и сохраняющиеся за счет неразвитости, рассогласованности системы регуляторов поведения, связанные с личностными свойствами индивида, а также с окружающей средой, которая в форме повторяющихся конкретных жизненных ситуаций представляет возможность для их проявления и реализации, в том числе и в виде отклоняющегося поведения»[85]. Анализ этих представлений имеет теоретическое и практическое значение.

Особое значение в деятельности органов внутренних по профилактике преступлений имеют условия нравственного формирования лиц, совершивших преступление в сфере цифровых технологий, в особенности среди ближайшего бытового окружения, связей, знакомств. Для предотвращения преступления исключительно важно выявить криминогенные обстоятельства конкретной жизненной ситуации, влияющей с учетом особенностей личности на возможность совершения преступления. Но решающим является знание социальных, психологических и нравственных свойств личности цифровых преступников (взгляды, навыки, привычки, содержание и уровень интересов и потребностей, особенности характера и др.). Криминологические данные о видах (к примеру: стафферы,

[85] *Саркисов Г.С.* Объект индивидуального профилактического воздействия в теории предупреждения преступности. Ереван, 1975.

заливщики, дроповоды, фишеры и др.) и типах (к примеру, с политической мотивацией; с корыстной мотивацией; с насильственно-эгоистической мотивацией; с анархическо-индивидуалистической мотивацией; с легкомысленно-безответственной мотивацией и т. п.) личности этих преступников выверены в научно-практических исследованиях, они базируются на широких обобщениях, анализе не только отдельных лиц, но и всего того общего, типичного, чем эти преступники выделяются в социуме. В этом отношении криминология имеет определенные рекомендации, применяет разнообразные методы и в результате получает достоверную информацию, которую необходимо использовать органам внутренних дел. Данная информация помогает познать механизм преступного поведения, который является объектом профилактического воздействия. На основе таких знаний сотрудники ОВД, сталкиваясь с обстоятельствами, способствующими подготовке к преступлению, лишь по объективным данным уже могут определить признаки и тип личности – преступника и определить примерную программу профилактического воздействия.

В рамках обозначенного направления изучаются лица: неоднократно совершавшие цифровые правонарушения и преступления, а также те, чьи личностные качества свидетельствуют о большой вероятности совершения таких преступлений. Механизмы и способы выявления последней категории лиц и оказание на них индивидуально-профилактического воздействия представляется в настоящее время центральной в деятельности специальных оперативных подразделений МВД России.

Анализируя вопросы теоретического и прикладного значения оперативной профилактики как наиболее перспективного направления предупреждения цифровых преступлений, рассмотрим ее как комплекс мероприятий, осуществляемых с использованием средств и методов оперативно-розыскной деятельности[86] направленных на решение определенных задач: устойчивую осведомленность о криминогенной части населения цифрового мира; своевременное получение сведений о тенденциях поведения криминально активных пользователях интернета; максимально возможное представление о системе антиобщественных и преступных связей в их среде; определение и анализ микросреды и сферы общения, продуцирующих антиобщественное и преступное поведение (очагов активного действия детерминант преступности); изобличение в этой среде

[86] *Овчинский С.С.* Оперативно-разыскная профилактика: лекция. Калининград: ВШ МВД СССР, 1982.

латентных преступников; анализирование социально-демографических и нравственно-психологических качеств лиц, поведение которых отражает антиобщественную направленность и указывает на возможность совершения цифровых преступлений.

Первоочередными задачами оперативной профилактики цифровых преступлений являются – «контроль и профилактическое воздействие» на лиц «замышляющих либо подготавливающих цифровые преступления», «состоящих на оперативно-разыскных и профилактических учетах ОВД». Оперативная профилактика, предотвращение и пресечение преступлений невозможны без воздействия на лиц, которые в силу своих отрицательных особенностей обладают потенциальной предрасположенностью к совершению цифровых преступлений.

Такая криминологически значимая информация о личности цифрового преступника является системообразующим элементом характеристики отдельных видов цифровых преступлений и позволяет разработать вероятностный прогноз развития преступной деятельности.

В деятельности органов внутренних дел обязательно применяется криминологическое прогнозирование индивидуального и группового преступного поведения. Такое прогнозирование становится возможным потому, что преступное поведение связано с объективными явлениями социальной среды многими нитями[87].

Прогнозирование составляет основу профилактического учета, так как его банки информации создаются на основе прогноза вероятности преступного поведения разных типов цифровых преступников. Информация о прошлом (судимость, правонарушения, аморальные проступки) и настоящем (поддержание отрицательных связей, паразитизм, склонность к виртуальному миру) поведении личности является основанием для прогностических выводов о возможном противоправном поведении в будущем. Учитываются варианты поведения, моральные и нравственные стереотипы лица, представляющего интерес. Совокупность обозначенных данных о лице является элементом, заложенным в метод криминологического прогнозирования, который используется в органах внутренних дел.

Таким образом, анализ криминологической информации о личности преступника является необходимой частью познавательного процесса в ходе расследования преступления или организации его

[87] *Калашников И.В.* Организованная преступность с участием несовершеннолетних и проблемные вопросы ее предупреждения // Вестник Московского университета МВД России. 2011. № 4.

предупреждения, который может быть представлен в виде криминолого-информационного процесса познания характеристик личности преступника субъектом органа внутренних дел.

Именно органы внутренних дел, владея информацией о намерении лица совершить преступления, обладают большими профилактическими возможностями и именно они могут выступить в качестве такого внешнего обстоятельства, которое заставит человека отказаться от преступного замысла и осознать необходимость корректировки своих жизненных позиций.

Личность преступника является носителем причин совершения преступления, она является основным и важнейшим звеном всего механизма преступного поведения, и, соответственно, ее особенности, которые порождают такое поведение, являются непосредственным объектом профилактического воздействия органов внутренних дел.

5.2. Структура личности, совершившей преступление в сфере цифровых технологий

Статистика свидетельствует о том, что количество цифровых преступлений ежегодно растет. Современный криминальный мир уже не мыслит своего существования без цифрового мира. Учитывая новизну и разнообразие цифровых преступлений, познание личности преступника приобретает особую актуальность, поскольку дело приходится иметь с субъектами, ранее не попадавшими в поле зрения правоохранительных структур.

При изучении личности, совершившей преступление в сфере цифровых технологий, необходимо исходить из следующих постулатов:

– совокупность интегрированных в личности преступника социально-значимых свойств образуется в процессе многообразных и систематических взаимодействий с другими людьми. Этот аспект личности позволяет рассматривать личность преступника как: члена общества; социальных / антисоциальных групп или иных общностей (например, студент технического вуза, член хакерской организации «Анонимус» и т. п.); носителя социально-типичных черт;

– человек не рождается, а становится преступником;

– изучению подвергаются все субъекты совершения самых разнообразных цифровых преступлений, в том числе и занимающих малую долю;

– антиобщественные взгляды, ориентации и ярко выраженная индивидуалистическая направленность не характерна всем без исключения лицам, совершившим цифровое преступление;

– личность преступника отличается от законопослушной личности своей общественной опасностью. Однако общественная опасность личности гражданина не предполагает фатальности преступного поведения. Это качество либо реализуется, либо не реализуется в его деятельности, что зависит как от самой личности, так и от внешних обстоятельств, способных препятствовать такому поведению.

Указанное позволяет нам на основе официальных статистических данных выявить типичные компоненты структуры личности преступника.

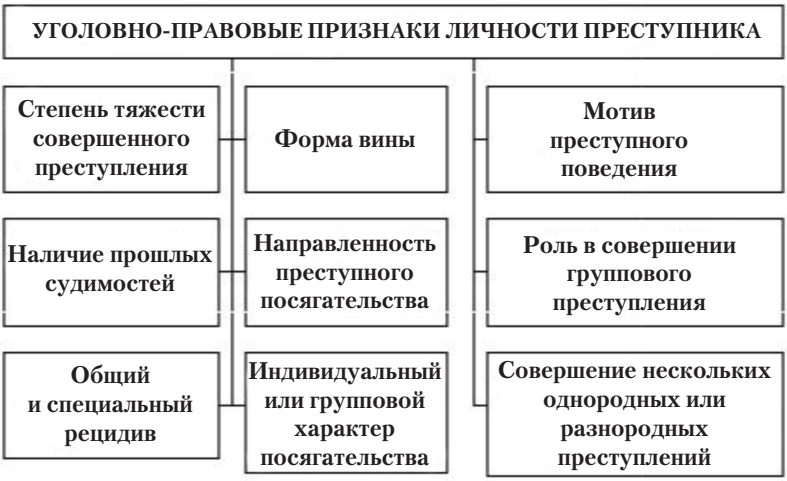
Структура личности преступника – это значимое с точки зрения криминологии упорядоченное соотношение свойств индивида, которые характеризуют лиц, совершивших уголовно наказуемое деяние.

В обычном понимании принято считать, что цифровые преступления совершают высококвалифицированные программисты, спе-

циалисты в области телекоммуникационных систем, – профессионалы. Однако в общем объеме всех цифровых преступлений такой вид профессионалов занимает незначительную долю. Обобщенная характеристика цифрового преступника базируется на официальных статистических данных выявленных лиц, совершивших разнообразные цифровые преступления.

В структуре личности преступника выделяется ряд подструктур. Различные ученые выделяют различные подструктуры. Мы остановимся на наиболее простой классификации личностных свойств, согласно которой все основные составляющие личности можно разделить на три группы:

1. Уголовно-правовая характеристика – совокупность данных, которые свидетельствуют о начале виновным преступной карьеры или о ее продолжении. При сборе информации в рамках данного блока структуры личности преступника ключевыми элементами выступают признаки состава преступления. Таким образом, данная характеристика включает себя сведения о тяжести совершенного преступления, форме вины, мотивах преступления, место и роль в совершении преступления, имеются ли судимости, привлечения к уголовной ответственности, форма рецидива и др.

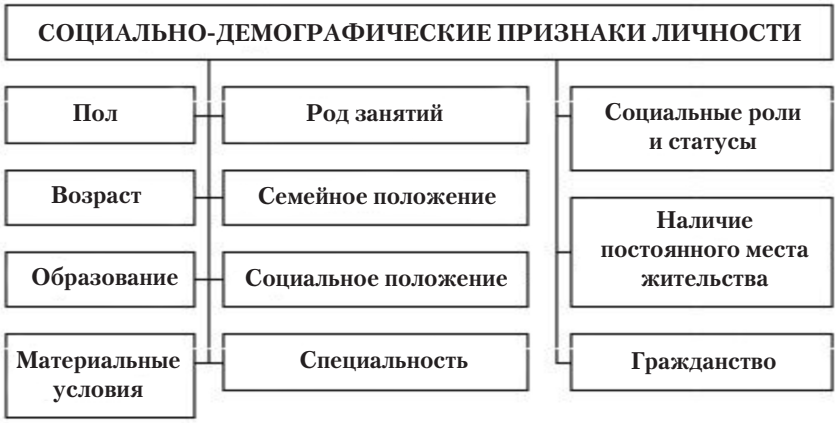


Необходимо отметить, что цифровые преступления умышленные, в большинстве спланированы. Всего 6 % лиц имели психические отклонения, не исключающие вменяемость. Лиц, признанных невменяемыми, среди цифровых преступников нет. Доля совершив-

ших преступление в состоянии алкогольного опьянения небольшая и составляет 18 %. 80 % лиц совершали преступления единолично, лишь 15 % группой лиц, по предварительному сговору.

Особую тревогу вызывает факт, что 50 % этих преступников ранее совершали различные преступления, 10 % из которых имели рецидив преступлений, совершили преступление при условном осуждении, в течение года после освобождения из мест лишения свободы, состояли под административном надзором, а 25 % были заключены под стражу. Это указывает на заинтересованность преступного элемента совершения корыстных преступлений в цифровой сфере, общеуголовный элемент переквалифицируется с «обыденных» для них преступлений в «высокотехнологичные», совершенствуя ранее полученные преступные навыки. Такая группа цифровых преступников отличается криминальной устойчивостью и профессионализмом.

2. Социально-демографическая характеристика – это сведения о поле, возрасте, образовательном уровне, материальных условиях, семейном положении. Отдельно в этом блоке выделяют социально-ролевую характеристику преступника – социальный статус, социальные функции (профессия, профессиональная принадлежность, род занятий) и др.



Цифровые преступления совершают как мужчины (75 %), так и женщины (25 %), в основном в возрасте 30–49 лет – 45 % и 18–24 – 25 %, что позволяет сделать вывод о сформировавшемся характере личности цифрового преступника. Имеют оконченное средне-профессиональнее образование – 35 %, среднее (полное)

общее – 32 %, учащиеся – 5 %, работники коммерческих или иных организаций – 12 %, без постоянного источника доходов – 55 %. Граждане России – 96 %.

3. Нравственно-психологическая характеристика – выражение отношения преступника к обществу в целом, принятым в нем ценностям и нормативно-одобряемым социальным ролям. В данную характеристику входят: интеллект, способности, навыки, привычки, волевые и эмоциональные установки, интересы, ценностные ориентации, отношение к нормам морали и права, потребности, избираемые способы удовлетворения потребностей и др.

Среди ценностных ориентаций у данной категории лиц преобладают индивидуально – и клановo-эгоистические. В данных случаях доминируют желание материального благополучия, наиболее комфортных условий, проявления своего эго либо клановo-эгоистический интерес.

Нравственное и правовое сознание личности у компьютерных правонарушителей обычно деформировано или ослаблено.

Корыстные мотивы порождаются гипертрофированными или извращенными потребностями, к примеру стремлением к легкой наживе. Доли молодых людей, которые составляют 25 % цифровых преступников, свойственны также потребности социального характера, что ведет к формированию мотивов агрессивной окраски. Они имеют трудности общения со сверстниками, противоположным полом, ищут самореализацию в виртуальном мире, «замкнуты

и скрытны», но при этом «стремятся к самоутверждению, желают получить известность, приобрести авторитет в своем кругу». Наряду с корыстными мотивами, распространены, хулиганские, политические, игровые, исследовательский интерес, потребность в самоутверждении, месть, мотивы, связанные с психическими отклонениями. Мотивами преступных действий несовершеннолетних обычно являются исследовательский интерес, самоутверждение и жажда славы.

Несмотря на приведенные данные о типичном образе преступника, совершившего преступление в сфере цифровых технологий, мы полагаем, что он меняется. Представление о них как об инфантильных, субтильных, замкнутых, склонных к депрессиям, а также всевозможным злоупотреблениям, небрежно выглядящих молодых людях устарело. Сейчас быть цифровым преступником модно, прежде всего, из-за материальной выгоды. В результате в цифровую преступность потянулись общеуголовные преступники, а также предприимчивые, авантюристичные и даже харизматичные люди, которые могут получить крупные преступные доходы, с большой вероятностью избежав при этом уголовной ответственности.

Следующим шагом на пути научного осмысления проблемы личности преступника является обобщение и систематизация ее свойств и качеств.

В юридической литературе в зависимости от характера систематизации лиц, совершивших преступления, выделяют классификацию и типологию преступников. Таким образом, классификация и типология, при всей их схожести, не одно и то же.

Классификация, являясь более низким уровнем обобщения, представляет собой устойчивую группировку исследуемых объектов по их отдельным признакам и строится на весьма жестких критериях групп и подгрупп, каждая из которых занимает четко зафиксированное место. Типология такой жесткой дифференциации не содержит.

По мотивам совершения цифрового преступления (или иначе по характеру общественной опасности) можно выделить наиболее распространенные типы личности цифрового преступника:

– корыстный тип (объединяет всех лиц, совершивших цифровые преступления по мотивам личного обогащения);

– престижный тип (лица, совершающие преступления из престижных побуждений, т. е. для того, завоевать авторитет среди окружающих, быть все время на виду и т. д.);

– насильственный тип (данный тип цифрового преступника заключаете в совершении психического насилия в отношении лиц: ревность, завесить и т. п., однако их доля невелика).

– сексуальный тип (характерен для лиц, виновных в распространении порнографии в Интернете и получении от этого удовлетворения)

Разумеется, могут быть выделены и другие типы.

Исходя из критерия социальной направленности личности цифрового преступника можно выделить:

Профессиональный тип. Самый опасный тип. Направленность личности деформирована и представлена в виде негативной направленности. Для этого типа характерна внутренняя тяга к совершению повторных преступлений, он активен в нахождении и создании собственными усилиями ситуаций, способствующих совершению преступлений.

Привычный тип. Для него характерна значительная деформация в структуре социальной направленности, позитивный компонент слабо выражен. От профессионального типа отличается тем, что для совершения преступления преимущественно использует различные жизненные ситуации; не активен в самостоятельном создании таких ситуаций.

Неустойчивый тип. Компоненты негативной и позитивной направленности примерно равны, но тенденции у них противоречивы. До преступления возможны различные правонарушения или аморальные действия.

Небрежный тип. Социальная направленность данного типа в основном выражена позитивным компонентом, негативная направленность минимальная. Характеризуется легкомысленным отношением к социальным нормам.

Случайный тип. Характеризуется позитивной социальной направленностью. Без деформаций со стороны негативного компонента. Преступление совершает исключительно в силу давления критической жизненной ситуации.

В практической деятельности по предупреждению преступлений учет личностного фактора играет едва ли не решающую роль, которая проявляется в следующих основных направлениях: при статистическом анализе преступности по лицам, при изучении причин и условий совершения конкретных преступлений, при проведении индивидуальной профилактической работы сотрудниками органов внутренних дел, при назначении наказания судами, в оперативно-розыскной деятельности.

Контрольные вопросы

1. Назовите основные направления ОВД, в которых необходимы знания о личности преступника, совершившего цифровое преступление.
2. Охарактеризуйте социально-демографические признаки личности преступника, совершившего цифровое преступление.
3. Определите основные характеристики уголовно-правовой составляющей личности преступника, совершившего цифровое преступление.
4. Охарактеризуйте нравственно-психологические признаки личности преступника, совершившего цифровое преступление.

Глава 6. Мониторинг, прогнозирование и планирование предупреждения цифровой преступности

Планируемые результаты освоения темы главы

– **знать** понятие мониторинга цифровой преступности, ее прогнозирования, а также направлений прогнозирования, а именно прогнозирования криминологических рисков и угроз, планирования предупреждения цифровой преступности;

– **уметь** применять свои знания для понимания закономерностей и тенденций развития цифровой преступности; проведения мониторинга; использовать методы криминологического прогнозирования (экстраполяция; метод экспертных оценок; моделирование), подготовить предложения для планирования предупреждения цифровой преступности;

– **владеть** терминологией мониторинга, прогнозирования, и планирования цифровой преступности; навыками для организации и проведения криминологических исследований; прогнозирования цифровой преступности, планирования профилактических мероприятий.

6.1. Роль мониторинга в деятельности ОВД по предупреждению цифровой преступности

Для правового государства проведение мониторинга выступает одним из способов обеспечения соблюдения законности правоприменительными органами и их должностными лицами. Изучение тех или иных особенностей в любом государственном строе и с учетом времени проводимой социальной политики всегда требует их толкования с различных позиций.

Результаты проведенных мониторингов требуют не только пересмотра нормативно-правовых актов, но и изменения деятельности субъекта правоприменения, тем более в области обеспечения безопасности, государственного управления и правоприменительной деятельности. Вместе с тем результаты мониторинга, которые требуют существенных изменений нормативно-правовых актов, структуры органов и т. п., должны обязательно оцениваться с научно-практических позиций.

Мониторинг как комплексная и плановая деятельность, может осуществляться федеральными органами исполнительной власти и органами государственной власти субъектов Российской Федерации в пределах своих полномочий, а также и общественными организациями, в том случае, когда юридическому лицу необходимо собрать, обобщить и анализировать необходимую для осуществления его деятельности информацию. В итоге мониторинговая политика (оценочная, правоприменительная) сегодня проводится в отношении всех (всеми) субъектов управления, в том числе и на низовых уровнях – местных и муниципальных, сельских поселений. Но, с другой стороны, по мнению авторов, мониторинговую политику в деятельности полиции следует рассматривать с государственно-надзорной точки зрения. Так, например, Генпрокурор РФ и подведомственные ему территориальные органы, осуществляя надзор по тем или иным направлениям деятельности полиции, дают оценку как НПА ОВД РФ, так и отдельным правоприменительным действиям, например, применению физической силы, огнестрельного оружия, отдельных норм КоАП и УК, УПК РФ и т. д.

Оценка непосредственной деятельности полиции (служб, подразделений) по реализации соответствующих нормативно-правовых актов уполномоченными лицами (госорганами) конкретного субъекта управления рассматривается как правоприменительный мониторинг. Он проводится как непосредственным субъектом управления (правоприменения), так и лицами, обладающими компетенциями для осуществления надзора и контроля. Полиция обладает также государственно-надзорными и контрольными функциями по определенным направлениям. Здесь мониторинг выступает как один из способов обеспечения законности и должной административной деятельности полиции по тем или иным направлениям. При этом его результаты могут применяться на практике и позволят разработать стратегию и тактику противодействия преступности.

В такой деятельности необходимо использовать современные методы контроля и анализа при мониторинге. Особое предпочтение должно быть отдано технологии больших данных. Речь идет уже о существующих инструментах, методах и программах интеллектуального анализа структурированных и неструктурированных данных (больших данных) для практического перехода к вычислительной криминологии. Известно, что задача правоохранительных органов, предупредить, предотвратить, пресечь любую преступную деятельность. Следовательно, необходимо проводить мониторинг на более ранней стадии, возможно на стадии подготовки преступ-

ной деятельности. Здесь следует вспомнить и о криминологическом мониторинге.

Криминологический мониторинг это «система социально статистического наблюдения, позволяющая устанавливать показатели преступности, уровень ее латентности, социальные последствия, выявлять ее причины и условия, прогнозировать их развитие в будущем, принимать адекватные государственные и общественные меры по предупреждению преступности и устанавливать их эффективность».

Основной целью мониторинга является определение реального состояния криминологической безопасности, установление показателей и оценки эффективности деятельности правоохранительных органов по предупреждению преступности. При этом следует иметь в виду, что такой вид мониторинга находит применение повсеместно и затрагивает в изучении не только основные показатели преступности, но и административную практику, оперативную обстановку, экономические, политические процессы в обществе, негативные социальные явления, оказывающие непосредственное влияние на преступность. При его проведении немаловажным является исследование общественного мнения, складывающейся социально-психологической обстановки в обществе, уровня социальной напряженности среди населения. В совокупности это предопределяет перечень мониторинговых показателей, которые требуется учитывать при проведении исследования данного вида преступности.

Таким образом, необходимость проведения криминологического мониторинга обусловлена:

– изучением цифровой преступности с целью определения антикриминальных механизмов противодействия этому виду преступности;

– определение направления по повышению эффективности деятельности правоохранительных органов в названной сфере.

Первостепенной задачей криминологического мониторинга является определение реальных показателей преступности и методов получения данных, позволяющих рассчитать эти показатели, в том числе и количественного, который позволяет изучить современное состояние цифровой преступности. Однако, учитывая то, что предмет исследования (цифровая преступность) является явлением еще не изученным и трудно выявляемым из-за высокой латентности, а также из-за проблем организационно-технического характера, в ходе мониторинга сложно определить инструментарий изучения. Во-вторых, в ходе исследования необходимо уделять внимание изучению уровня латентности цифровых преступлений,

с учетом видов латентности (естественной (объективной; искусственной, пограничной).

Более того, результаты изучения цифровой преступности свидетельствуют о том, что в большей части они совершаются в соучастии организованными группами и преступными сообществами и их изучение осложняется тем, что они пытаются избежать любого, а тем более количественного изучения. При этом следует иметь в виду, что организованная преступность не поддается изучению.

В связи с этим требуется особый подход к ее изучению, который позволит разработать критерии их изучения с использованием искусственного интеллекта оценить достоверность текстовой и аудиовизуальной информации, полученной в ходе предварительного и судебного следствия. Большое внимание в проведении мониторинга должно быть отведено использованию технологии больших данных, благодаря которой можно исследовать большую массу как структурированных, так и неструктурированных данных, выделив из них не столько «источники заслуживающие доверия и фейковые, сколько провести разделение по критериям достоверности не самих по себе источников, а содержащейся в них информации о персонах, событиях, ситуациях, организациях и т. п.»[88].

И здесь следует согласиться с мнением В. С. Овчинского, который считает, что для этого необходимо «создание удобного концептуального инструмента для описания тех или иных сфер и, главное, являются основой для разработки прогностического инструментария. В конечном счете работники правоохранительных органов ждут сегодня новые прогнозные инструменты[89].

Одним из основных механизмов обеспечения криминологической безопасности, можно считать мониторинг факторов, определяющих криминологические угрозы. Так, в современных условиях необходимо получение сведений о результатах мониторинга социально-экономического развития[90], социально-экономической и социально-политической ситуации в стране. Особое внимание следует уделять исследованию преступности и проблемным вопросам противодействия ей и прогнозу на ближайшие 3–5 лет. Полученные результаты исследования позволят определить прогноз

[88] Сборник избранных лекций по криминологии / под ред. д-ра юрид. наук, профессора Т. В. Пинкевич. Москва: Юрлитформ, 2020. С. 138.

[89] *Там же*.

[90] О проведении мониторинга прогноза социально-экономического развития Российской Федерации на 2019 год и на плановый период 2020 и 2021 годов: письмо Минэкономразвития России от 5 октября 2018 г. № Д14и-1974. Доступ из справ.-правовой системы «КонсультантПлюс».

изменения структуры противоправных проявлений и выявить особенности воздействия развития цифровых технологий на изменения, происходящие не только в экономической, политической и социальной сфере, но и в структуре преступности. Но кто и как должен проводить такой мониторинг?

Постоянный мониторинг в соответствие с законом РФ «Об основах системы профилактики правонарушений в Российской Федерации»[91] в сфере профилактики правонарушений как особый комплекс мероприятий, направленных на получение полной информации о состоянии профилактики правонарушений, проводится МВД России в субъектах РФ, но единого комплексного исследования, которое бы объединило все показатели преступности, определило причинный комплекс и пути снижения уровня криминологических угроз и рисков, нет. Статистические отчеты, которые представлены на сайтах правоохранительных органов не отражают полной картины криминогенной ситуации в стране. Зачастую исследуются только статистические показатели, зарегистрированной преступности, в редком случае – указывается ущерб. Пришло время отказаться от такого рода мониторинга и осуществлять анализ, основой которого должны стать, результаты работы с использованием методов и программ искусственного интеллекта, анализа больших данных и математико-статистических методов[92]. Такая подготовка должна вестись совершенно на новом методологическом уровне. Но для этого необходимо а) создание единой базы данных по преступности, которая будет ориентирована на машинную обработку данных и количественный анализ, что позволит «используя одни фрагменты данных, извлекать более глубокие выводы из других, казалось бы, не связанных с первыми, баз сведений»[93]; в) пополнение базы данных открытых исследований преступности, внутренней статистикой правоохранительных органов, при этом провести разделение по критерию достоверности информации о событиях, ситуациях, персонах, организациях и т. п.; г) дополнение информацией о деятельности общественных приемных, молодежных и вете-

[91] Об основах системы профилактики правонарушений в Российской Федерации: федер. закон от 23 июня 2016 г. № 182-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

[92] *Овчинский В.С.* Как изучать организованную преступность в XXI веке [Электронный ресурс]. URL: https://izborsk-club.ru/15222 (дата обращения: 05.08.2020).

[93] Например, в 2016 г на конференции в Академии ФБР было принято решение о создании такой базы в рамках программы ФБР на 2015–2025 гг. «Искусственный интеллект против криминала» (см. Овчинский В.С. Как изучать организованную преступность в XXI веке [Электронный ресурс]. URL: https://izborsk-club.ru/15222) (дата обращения: 18.03.2021).

ранских организаций, учебных заведений, а также результатами мониторинга в интернет-среде; д) уделить особое внимание анализу и прогнозированию преступности с ее региональным аспектом личности преступника, причинного комплекса с целью прогнозирования и противодействия тем новым вызовам криминологической безопасности, которым необходимо противостоять.

Если весь названный массив информации постоянно пополнять и анализировать с учетом новых цифровых технологий, то, по мнению В. С. Овчинского «будет сформирован беспрецедентный массив информации о преступности»[94], который, как представляется, должен быть основным материалом для оперативно-розыскной деятельности правоохранительных органов и вспомогательным материалом для повышения качественной и эффективной деятельности всех субъектов профилактики. Именно результаты такой деятельности должны быть положены в основу подготовки целевых программ по противодействию преступности.

В ходе мониторинга особое значение будет иметь получение финансовых данных обо всех учредителях, финансовых показателях, руководстве юридических и финансовых лиц, об их транзакциях и упоминании в средствах массовой информации и пр.

Нельзя забывать и о тщательном изучении текстового контента, который может быть размещен как в информационных, так и в телекоммуникационных сетях, поскольку перед совершением, например, террористических актов в 85 % случаев в интернете появлялась та или иная необычная информация, которая при должном к ней внимании могла помочь предотвратить преступление или теракт.

При этом, следует отметить, что при изучении криминальной ситуации на любом уровне, необходимо в обязательном порядке исследовать результаты мониторинга других ведомств и учреждений, поскольку очень часто в ним можно найти необходимую информацию для противодействия латентной преступности, а также при определении уровня социальных последствий.

---

[94] *Овчинский В. С.* Как изучать организованную преступность в XXI веке [Электронный ресурс]. URL: https://izborsk-club.ru/15222 (дата обращения: 22.06.2020).

6.2. Прогнозирование цифровой преступности

Одной из функций криминологии является прогностическая функция, представляющая собой разновидность социального предвидения, а точнее, речь идет о научном предвидении в сфере противодействия преступности. Именно прогнозирование позволяет с учетом результатов наблюдения, изучения законодательной базы и определения наступления состояний, детерминирующих преступные проявления, путем экстраполяции, моделирования либо экспертной оценки, прогнозировать свойства преступных проявлений в будущем.

По мнению профессора В.В. Лунеева, криминологическое прогнозирование представляет собой научное предсказание основных изменений (тенденций) развития преступности или вероятности совершения уголовно-наказуемых деяний конкретными лицами в обозримом будущем, базирующееся на исследованиях, проводимых научными и практическими сотрудниками. Оно основывается на знании тенденций преступности, а также на разнообразных и взаимосвязанных процессах, оказывающих непосредственное влияние на криминальную и антиобщественную среду. Анализ количественных и качественных характеристик преступности в прошлом и настоящем позволяет установить общие закономерности развития этого социально-негативного (общественно-опасного) явления в будущем. Обычно рассматривают два направления прогнозирования: криминологические угрозы и криминологические риски.

Отличия криминологического прогнозирования от иных видов прогностики: 1) высокая интенсивность связи между прогнозом и управленческими решениями; 2) криминологическое прогнозирование является составной частью прогнозирования социального, поэтому носит условный характер и содействует повышению объективности и эффективности деятельности субъектов профилактики и уголовного судопроизводства; 3) предсказания основываются на двух типах прогнозов: а) поисковых–уточнение и целевые явления возможных изменений тенденций преступности в ближайшей перспективе; б) нормативных – определение альтернативных, либо оптимальных способов разрешения криминогенных проблем на основе существующих критериев социума.

При криминологическом прогнозировании цифровой преступности перед исследователями стоит задача выявления «тенденций и закономерностей возможного развития преступности, пове-

дения конкретных лиц или других криминологически значимых процессов»[95].

При осуществлении такой деятельности необходим:

– сбор прогностически значимых показателей цифровой преступности, включающих информацию о развитии и внедрении цифровых технологий, об их положительных и отрицательных качествах, о влиянии их внедрения на социальные процессы в обществе (миграция, безработица и пр.), о развитии законодательства и пр. Вся полученная информация должна быть собрана, структурирована и систематизирована по показателям будущей преступности;

– разработка методик криминологического прогнозирования названной преступности, которые смогут использоваться в практической работе сотрудники правоохранительных органов;

– предсказание вероятности трансформации показателей преступности в зависимости от текущих изменений причин и условий, детерминирующих криминальные явления (социально-политических, социально-экономических и пр.);

– разработка математического и технического инструментария, с помощью которого возможно предсказать вероятность массового совершения преступных деяний на определенной территории за период времени.

Для криминологического прогнозирования необходимы такие прогностические показатели, как:

– региональные или муниципальные показатели социально-демографических и социально-экономических закономерностей развития общества;

– причины и условия, способствующие совершению цифровых преступлений**;**

– результаты оценки современного состояния цифровой преступности за прошедшие годы и в настоящее время;

– причинный комплекс цифровой преступности прошлого периода (берется промежуток времени аналогичный промежутку изучения преступности и настоящего, которым свойственны экономические и социальные явления, связанные с преступностью).

Виды криминологического прогнозирования различаются:

– по продолжительности периода упреждения: а) оперативный до 1 месяца; б) краткосрочный до 1 года; в) среднесрочный до 5 лет; г) долгосрочный от 15 до 20 лет;

– по способу решения задач, стоящих перед прогнозом:

---

[95] Криминология: учебник для академического бакалавриата / В.В. Лунеев. Москва: Юрайт, 2019.

а) оперативные – используются в повседневной деятельности правоохранительных органов;

б) тактические – служат для формирования перечня приоритетных направлений деятельности правоохранительных органов;

в) стратегические – используются в управленческой сфере для определенных целей борьбы с преступностью.

– по признаку сложности объекта прогноза:

а) простой (однообъектный), когда объекты изолируются от структуры внешних связей;

б) факторный– когда прогнозу подвергается множество явлений;

в) системный – когда учитываются уровни, направления прогнозируемых объектов, теснота взаимосвязи, пространственно-временные и социально-психологические параметры;

г) математический – когда для создания системы посредством математических расчетов создается модель проектируемой системы.

– по методу криминологического прогнозирования.

При этом в криминологии на современном этапе развития науки и практики используется ряд основных прогностических методик, которые применимы для предвидения тенденций преступности. К ним следует отнести экстраполяцию, системный метод, метод экспертных оценок и моделирования. Благодаря их применению могут разрабатываться краткосрочные (до 1 года), среднесрочные (до 5–10 лет) и даже долгосрочные (до 15 и более лет) прогнозы. Так, например, использование метода экстраполяции позволяет изучать данные прошлых лет о преступности и их современное состояние для того, чтобы выявить ее будущие тенденции. При этом, полученные выводы могут иметь как общий анализ преступности, так и дифференцированный по видам и группам, но следует иметь в виду, что данный метод следует использовать при краткосрочных прогнозах.

Второй метод, системный анализ, который позволяет определить взаимосвязь роста преступности, ее причин и условий с различными социальными факторами.

Следующий метод – метод экспертной оценки, в основе которого лежит опросник. С его помощью и осуществляются сбор требуемой информации, аналитическая информация, экспертные оценки по изучаемой проблеме. Получение экспертных прогностических заключений возможно следующим способами: а) свободное интервью – мнение специалиста криминолога; б) мозговая атака – коллективное заключение по рассматриваемой проблеме экспертов; в) аналитические экспертные оценки– это письменные заключения

определенных специалистов по криминогенной ситуации; г) метод Дельфи –многократный анкетный опрос одной и той же группы экспертов с применением шкалированных оценок.

И, метод моделирования, который применяется при необходимости исследования будущего криминального явления посредством построения модели реально существующего процесса для изучения его будущих качественных и количественных характеристик с целью получения новых знаний о предмете. В криминологии используется метод имитационного моделирования, когда качественная и количественная информация об исследуемом объекте искажается в минимальной степени, с сохранением возможности точного отображения динамики изменений состояния объекта на некотором временном периоде.

Особая значимость в прогнозировании отводится исследованию и определению криминологических рисков и угроз, результаты исследования которых должны быть положены в основу планирования деятельности органов внутренних дел. В ходе криминологического прогнозирования особая роль отводится исследованию рисков современного общества, в котором проявления человеческой активности либо «сознательно генерируют, либо допускают возможность наступления неких опасных и вредных последствий».

Раскрывая криминологические риски развитие цифровых технологий в России, следует отметить, что процессы внедрения индустрии цифровых технологий не только диктует новые правила, но и открывает недоступные ранее горизонты развития.

С внедрением цифровых технологий и результатов их деятельности, как свидетельствуют результаты прогноза, изменятся социально-экономические условия, в их числе рост количества таких преступлений, как мошенничество, преступления в сфере экономической деятельности. Особое место в этом ряду займут хакерские атаки. При этом особое внимание обращается на его непроизвольные автоматические реакции, которые и будут использоваться социальными инженерами при фишинговых атаках, использовании телефонии и т. п. Так, согласно аналитическому материалу, подготовленному ВНИИ МВД России совместно с Академией управления МВД России о росте числа преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, в данной сфере прогнозируется увеличение числа такого рода преступлений[96].

[96] Аналитический материал «Состояние преступности на территории Российской Федерации в условиях пандемии COVID-19 и тенденции ее развития до конца 2020 г.: ВНИИ МВД России, Академия управления МВД России, 2020.

Кроме того, к 2022 году практически на всех континентах будут широко использоваться беспилотные летательные аппараты, управляемые искусственным интеллектом. Использование дронов как юридическими, так и физическими лицами будет способствовать их массовой закупки преступниками и террористами, например, для транспортировки наркотиков и доставки взрывчатых веществ. Уже разработаны снайперские винтовки дальнего действия, с джойстиками для управления, которые заметно снизят требования к профессиональной подготовке боевиков. Вооруженный подобной винтовкой малообразованный и не имеющий боевого опыта человек по эффективности действий может соответствовать бывалому бойцу спецназа.

Вышеизложенное свидетельствует о том, что социальные последствия от внедрения цифровых технологий будут ощутимыми, поскольку преступность будет расти пропорционально количеству безработных, мигрантов и ущерба от преступности в целом.

Наиболее тесно с криминологическим прогнозированием связано Министерство органов внутренних дел РФ, которое должно формировать основные направления государственной политики в сфере внутренних дел на основе анализа и прогнозирования: состояния цифровой преступности. Органы внутренних дел обязаны при разработке ведомственных проектов нормативно правовых актов, проводить изучение информации, учитывая в том числе данные криминологических и социологических исследований, а также криминологических прогнозов. Приказ МВД России от 17 января 2006 г. № 19 «О деятельности органов внутренних дел по предупреждению преступлений» обязывает структурные подразделения центрального аппарата МВД России определять основные направления профилактической деятельности, осуществлять методическое обеспечение деятельности подразделений органов внутренних дел по предупреждению преступлений, комплексный анализ и прогнозирование криминогенной обстановки. Тот же самый приказ на окружном, межрегиональном и региональном уровнях устанавливает обязанность по проведению комплексного анализа и осуществление прогнозирования криминогенной обстановки.

Следующим механизмом обеспечения криминологической безопасности является прогнозирование социально-экономического, социально-политического развития общества и социальных последствий, с учетом факторов и процессов, угрожающих криминологической безопасности государства. В их числе речь должна идти и о научном предвидении в сфере противодействия преступности. Она позволяет на основе результатов наблюдений, изучения

закономерностей и тенденций, особенно криминологических закономерностей общественных отношений и результатов научно обоснованного криминологического прогноза, изучения законодательной базы и определения наступления состояний, детерминирующих преступные проявления, прогнозировать свойства преступных проявлений в будущем[97].

Нельзя также оставлять без внимания исследование социальных последствий цифровой экономики и внедрение цифровых технологий. Сегодня сложно представить какого уровня достигнет безработица при внедрении робототехник искусственного интеллекта, а то что уровень ее будет высоким не вызывает сомнений, так как многие считающиеся ранее профессиональными специалисты окажутся невостребованными в новых условиях. А на фоне продления срока выхода не пенсию такая ситуация приведет к еще большему расслоению общества и росту преступности. Это сразу скажется на уровне миграции, поскольку именно она является индикатором ухудшения социально-экономических, политических и экологических условий. При этом увеличится не только внутренняя, но и внешняя миграция, а численность нелегальных мигрантов будет возрастать.

[97] *Пинкевич Т.В.* Криминологические риски индустрии цифровых технологий в России // Криминальные реалии, реагирование на них и закон (Москва, 23–24 января 2018 г.) / под ред. А. И. Долговой. Москва, 2018.

6.3. Планирование предупреждения цифровой преступности

Предупреждение преступлений в современном урбанизированном и цифровом обществе невозможно без научно обоснованного планирования деятельности всех субъектов профилактики. Федеральный закон №182-ФЗ от 23 июня 2016 г. «Об основах системы профилактики правонарушений в Российской Федерации» определил, что реализация основных направлений профилактики правонарушений осуществляется посредством разработки государственных и муниципальных программ. Это разработка специальных целевых мероприятий федеральными органами государственной власти, органами исполнительной власти субъекта федерации и администрациями муниципальных образований, определяющих перечень профилактических мер, субъектов профилактики, сил и средств, участвующих в мероприятиях, механизмов реализации и финансирования, ожидаемых результатов с целью устранения или нейтрализации причин и условий правонарушений на определенной территории за конкретное время. Целью криминологического планирования является разработка и реализация конкретных профилактических мероприятий, основанных на научно определенных целях, задачах, ресурсах с целью разрешения социально-криминологических проблем. Задачи криминологического планирования состоят:

1) в координации совместной деятельности всех субъектов профилактики субъекта (города, муниципального района);

2) в реализации управленческой составляющей посредством вменения обязанностей должностным лицам, так как криминологические планы (планы предупреждения преступлений (правонарушений)) являются нормативно-правовыми актами ведомственного, регионального и муниципального значения;

3) в устранении или нейтрализации причин и условий правонарушений на определенной территории за конкретное время.

Разработка планов по предупреждению преступлений должна учитывать следующие обстоятельства:

1) региональные комплексные планы должны соответствовать федеральным, кроме того, региональным программам предупреждения преступлений, должны коррелировать с ведомственными планами правоохранительных органов субъекта, соответственно городские и муниципальные должны соответствовать краевым (областным, республиканским);

2) городские и муниципальные планы должны учитывать криминологические, социальные, культурные, религиозные особенности территорий;

3) планы профилактики правонарушений следует соотносить с планами социального и экономического развития регионов (городов, районов).

Выделяются следующие уровни криминологического планирования в структуре мер борьбы с преступностью: 1) общепрофилактические, связанные с социальным и экономическим развитием субъекта (города, района);

2) комплексные планы по противодействию преступлениям и правонарушениям в целом;

3) целевые планы предупреждения отдельных видов преступлений, либо «пограничных правонарушений».

Разработки планов по предупреждению преступлений и правонарушений должна учитывать следующие методические особенности:

1) разработка планов проводится руководителем государственного (муниципального) органа (учреждения), руководителями структурных подразделений, должностными лицами ответственными за организацию профилактики с учетом целей и задач, решаемых государственными (муниципальными) органами (учреждениями);

2) цель планирования должна быть связана с основной деятельностью государственного (муниципального) органа (учреждения), четко сформулирована и понятна всем участникам;

3) рекомендуется оптимальная продолжительность – это один календарный год, как оптимальная продолжительность, позволяющая осуществить контроль выполнения плановых мероприятий, либо провести их корректировку;

4) мероприятия формулируются с учетом прогноза, указываются этапы реализации плана и показатели, которые позволят оценить результаты ее реализации;

5) перечисление мероприятий профилактики правонарушений рекомендуется по нисходящей от общего к частному, с разделением по территориальному принципу, временному, по объекту посягательства, субъектам правонарушения и т. д.

Планы криминологического прогнозирования могут классифицироваться: а) по срокам действия; б) по масштабу; в) по назначению. Может быть предложена и иная классификация, например по видам планирования: 1) по продолжительности – оперативный до 1 месяца; б) краткосрочный до 1 года; в) среднесрочный до 5 лет; г) долгосрочный от 15 до 20 лет; по способу решения задач: а) оперативные – используются в повседневной деятельности правоохрани-

тельных органов, органов исполнительной власти и местного самоуправления; б) тактические – служат для формирования перечня приоритетных направлений деятельности правоохранительных органов, органов исполнительной власти и местного самоуправления; в) стратегические– используются в управленческой сфере для определенных целей борьбы с преступностью.

При этом в зависимости от продолжительности планируемой деятельности выделяют: перспективные, текущие, оперативные планы.

Итак, криминологическое планирование – это процессы разработки и реализации конкретных профилактических программ, основанных на научно определенных целях, задачах, ресурсах с целью разрешения социально-криминологических проблем. В целом такая деятельность должна способствовать не только выработке эффективных мер, направленных на предотвращение, пресечение, упреждение цифровых преступлений, но и совершенствованию системы предупреждения преступности. В настоящее время переход к цифровой экономике государства требуют не только объективной оценки прежней работы, критического анализа полученных результатов, но и выработки новых концептуальных идей и стратегических решений.

Криминологический мониторинг, прогнозирование и планирование обеспечивают не только определение оптимального варианта научно обоснованной стратегии и мер повышения уровня организаторской деятельности государственных и общественных органов, но и выработку тактики и методики борьбы с преступностью. Названные мероприятия в деятельности правоохранительных органов являются важным этапом планомерной борьбы с преступностью, ибо только на основе мониторинга, прогноза и планирования можно решать вопросы принятия заблаговременных решений относительно воздействия на преступность.

Контрольные вопросы

1. Дайте понятие мониторинга в сфере цифровых технологий и назовите его виды.
2. Дайте понятие криминологического прогнозирования цифровой преступности и перечислите его цели.
3. Определите роль прогнозирования цифровой преступности?
4. Какое значение в деятельности ОВД играет исследование криминологических рисков в связи с внедрением и разработкой цифровых технологий?

Глава 7. Предупреждение преступлений, совершаемых в условиях цифровой трансформации

Планируемые результаты освоения темы главы

– **знать** понятие предупреждения преступлений, уровни предупредительной деятельности, цели и задачи, особенности;

– **уметь** характеризовать предупредительные меры общесоциального характера и специально-криминологические, определять основные направления предупредительной деятельности;

– **владеть** терминологией категории «предупреждение преступлений», «профилактика преступлений», «выявление преступлений», «пресечение преступлений», навыками подготовки мер предупредительного характера.

7.1. Теоретические основы предупреждения преступлений, совершаемых в условиях цифровой трансформации

Криминологическая ситуация в России продолжает быть сложной, поэтому предупреждению преступлений уделяется особое внимание. Государством принимаются необходимые меры по изменению сложившейся ситуации и снижению напряженности в этой сфере. В связи с этим, на федеральном уровне принят ряд документов, который определяет основные принципы, задачи и цели предупреждения преступлений, как в целом, так и отдельных ее видов[98]. Это дает основание считать, что правовая основа предупреждения преступлений создана и действует единая государственная система их предупреждения.

[98] Концепция общественной безопасности в Российской Федерации (утв. Президентом Российской Федерации. 14 ноября 2013 г. № Пр-2685). Доступ из справ.-правовой системы «КонсультантПлюс»; Концепция противодействия терроризму в Российской Федерации (утв. Президентом Российской Федерации 5 октября 2009 г.). Доступ из информационно-правового портала «Гарант»; О противодействии терроризму: федер. закон от 6 марта 2006 г. № 35-ФЗ. Доступ из информационно-правового портала «Гарант»; О Стратегии национальной безопасности Российской Федерации: указ Президента Российской Федерации 31 декабря 2015 г. Доступ из справ.-правовой системы «КонсультантПлюс»; Обеспечение общественного порядка и противодействие преступности (утв. постановлением Правительства Российской Федерации от 15 апреля 2014 г. № 345). Доступ из информационно-правового портала «Гарант»; Об основах системы профилактики правонарушений в Российской Федерации: федер. закон от 23 июня 2016 г. № 182-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

Целью деятельности, направленной на предупреждение преступлений, совершаемых в сфере цифровых технологий, является снижение уровня этих преступлений, а также защита личности, общества и государства от преступных посягательств.

Основная задача предупреждения преступлений, совершаемых в сфере цифровых технологий, заключается в выявлении, устранении и нейтрализации причин и условий, способствующих совершению названных преступлений и предотвращении готовящихся преступлений.

Практическая реализация целей, задач и принципов предупреждения преступлений зависит от правоприменительной деятельности. Объектом предупредительной деятельности выступает система причин и условий, способствующих совершению преступлений, что дает основание рассматривать предупредительную деятельность как целенаправленная деятельность государства, общества, физических и юридических лиц, направленную на недопущение их совершения путем выявления, анализа, устранения или нейтрализации причин преступлений, условий, способствующих их совершению, оказания предупредительного воздействия на лиц с противоправным поведением[99]. Необходимо отметить, что понятие предупреждения преступности является родовым понятием по отношению к понятиям: профилактика предотвращение и пресечение преступлений. По мнению ряда авторов эти понятия идентичны[100].

При этом, профилактика преступлений – это предупредительная деятельность, направленная на устранение, ослабление, нейтрализацию криминогенных факторов, детерминирующих преступление; недопущение совершения преступления лицом, ведущим антиобщественный образ жизни; разъяснение гражданам их прав и обязанностей, способов защиты себя, своего имущества от преступных посягательств.

Под предотвращением преступлений понимается деятельность, направленная на недопущение замышляемых или подготавливаемых преступлений. На этой стадии формирования замысла преступного поведения путем проведения оперативно-розыскных мероприятий: выявляются лица, от которых по их негативному поведению можно ожидать совершений правонарушений (престу-

[99] Об основах системы профилактики правонарушений в Российской Федерации: федер. закон от 23 июня 2016 г. № 182-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

[100] Криминология: учебник для вузов / под ред В.Д. Малков. Москва: Юстицинформ, 2006.

плений); устраняются условия, которые способствуют реализации подобных мыслей.

Предупреждение преступлений, совершаемых в сфере цифровых технологий, требует весьма серьезных усилий государства и общества и может быть успешным только на основе использования широкого комплекса общесоциальных и специальных предупредительных мер.

Необходимой предпосылкой эффективности деятельности по предупреждению преступлений, совершаемых в сфере цифровых технологий является ее социальная и экономическая обоснованность. Вместе с тем предупредительная деятельность должна отвечать не только требованиям эффективности, но и системности. Системный подход к разработке и осуществлению мер предупреждения цифровых преступлений включает действия различных звеньев предупредительной деятельности, дифференцированных по масштабу, функциям, свойствам и в то же время взаимодействующих в решении задач предупредительного характера. Речь должна идти о всесторонности воздействия взаимосвязанного комплекса экономических, политических, социальных, правовых, идеологических и иных мер воздействия на причинный комплекс цифровой преступности.

В теории криминологии предлагается рассматривать систему предупредительного воздействия на преступность в четырех уровнях предупредительно-профилактической деятельности:

1) общесоциальное предупреждение, которое имеет целью устранение, нейтрализацию, ослабление всего комплекса криминогенных факторов; предупреждение самой возможности формирования антиобщественной направленности личности;

2) криминологическая профилактика, включающая устранение, нейтрализацию или ослабление неблагоприятных факторов социализации; пресечение начавшегося процесса криминогенной деформации личности; недопущение перехода на преступный путь лиц с явной антиобщественной направленностью; исключение рецидива со стороны лиц, уже совершивших преступления;

3) охранительное предупреждение преступлений удержание неустойчивых лиц от совершения преступлений; создание внешних, объективных препятствий, делающих невозможным или же затрудняющим совершение преступлений; обнаружение и пресечение подготавливаемых и начатых преступлений;

4) уголовно-правовое предупреждение, которое обеспечивает: механизмы общей и частной превенции с помощью устрашения уголовной ответственностью и практикой ее осуществления; лише-

ние лица с помощью изоляции физической возможности совершать преступления; исправительное и воспитательное воздействие в ходе отбывания наказания[101].

Построение системы предупредительно-профилактической деятельности можно считать оправданной, потому что она включает все этапы предупредительного воздействия. Следует признать, что в криминологической литературе предлагаются различные классификации предупредительных мер. Известно, что классификация мер предупреждения как прием научного исследования подчиняется строгим требованиям. Она должна, в частности, охватывать все меры, которые осуществляются субъектами предупредительной деятельности, обеспечить их исполнение и облегчить их применение, создавать теоретическую основу совершенствования методики их проведения, определить этапы проведения и т. п. Но все это возможно осуществить только при построении классификационных систем, основанных на различных критериях, а поскольку существует различные классификации предупредительной деятельности, остановимся на классификации предупреждения преступлений по уровню: общесоциальные и специально-криминологические предупреждение.

При этом общесоциальное предупреждение включает в себя совершенствование экономических, социальных, духовных, политических отношений в обществе; выявление и устранение диспропорций в них; криминологическая экспертиза; экспертные исследования, укрепление законности, социальная защита населения. На этом уровне наиболее эффективным является разработка социальных программ по отдельным проблемам криминогенного характера.

Основой общесоциального уровня предупредительной деятельности названных преступлений должны стать результаты проведенного мониторинга современного состояния цифровой преступности, при этом должны учитываться не только показатели зарегистрированных преступлений, совершенных в сфере цифровых технологий, но и реальное состояние с учетом ее латентной части, причинного комплекса, судебно-следственной практики по данной категории дел, механизма привлечения к уголовной ответственности и его реализация в целом, социально политической и экономической ситуации, сложившейся на момент подготовки мер предупредительного воздействия, результаты криминологического прогноза на краткосрочный и среднесрочный периоды, и другие составляющие, кото-

[101] *Устинов В. С.* Система предупредительного воздействия на преступность и уголовно-правовая профилактика. Москва, 1983.

рые позволят правильно и в полном объеме учесть все необходимые особенности современных криминологических угроз с целью определения направления предупредительного воздействия.

Специально-криминологическое предупреждение заключается в деятельности по предотвращению, пресечению и раскрытию преступлений; выявлению и устранению (нейтрализации) детерминант преступности, причин и условий конкретных преступлений; оздоровления социальной микросреды, коррекции поведения лиц, исправлению лиц, от которых можно ожидать совершения или уже совершивших преступления.

Социально-политические меры предупреждения преступлений, совершаемых в сфере цифровых технологий являются основными при осуществлении названной деятельности, так как государственная уголовная политика во «многом зависит от укрепления роли государственной власти, рационализации подходов к выработке решений в формировании уголовной политики, от создания условий для эффективной работы механизмов, основанных на саморегулировании и препятствующих развитию дестабилизирующих факторов»[102]. Важным направлением в данном случае должны стать меры, направленные на стабилизацию политической ситуации в России; укрепление и повышение авторитета политической власти; создание законодательной базы по охране цифровых технологий и защиты, но базы правовой защищенности российских граждан; выработка стратегии и тактики уголовной политики, а также политики идеологического воздействия.

К социально-экономическим мерам предупреждения преступлений, совершаемых в сфере цифровых технологий, следует отнести оздоровление экономики, укрепление кредитно-денежной системы государства как важнейшего института экономики, меры социальной защиты населения, в том числе повышение уровня жизни и др.

Меры социально-правового характера в период развития цифровых технологий очень важны, большое значение придается созданию законодательной основы, которая бы отвечала сегодняшним реалиям: принятие комплекса законодательных актов, внесение изменений в ряд действующих законодательных актов и нормативных документов, регулирующих создание и применение цифровых технологий, охрану общественных отношений, возникающих в связи с их применением и использованием в названной сфере, защиту

[102] Сборник избранных лекций по криминологии / под ред. д-ра юрид. наук, профессора Т. В. Пинкевич. Москва: Юрлитформ, 2020.

личности, общества и государства не только от их использования в быту и производстве, но и в преступных целях.

Особое внимание следует уделить и нормативным предписаниям, регламентирующим противодействие цифровой преступности, в соответствии с международно-правовыми стандартами и международными обязательствами России; заключение и ратификация международных Конвенций, межгосударственных договоров и соглашений по вопросам противодействия цифровой преступности.

Организационно-управленческие меры предупреждения преступлений, совершаемых в сфере цифровых технологий призваны способствовать организации предупредительной деятельности, принятию стратегических решений по обеспечению охранительными, контрольными и надзорными функциями органов и учреждений за сферой цифровых технологий, определить их взаимодействие по защите цифровых технологий от преступных посягательств и пр.

Предупреждение названного вида преступлений зависит от профессионализма субъектов предупредительной деятельности в сфере IT-технологий. В связи с этим необходима подготовка и переквалификация сотрудников правоохранительных органов, необходимо укрепление подразделений, которые непосредственно осуществляют мероприятия по противодействию преступлениям в сфере цифровых технологий.

Повышение эффективности предупредительной деятельности напрямую зависит от взаимодействия субъектов профилактики, деятельность которых должна быть скоординирована и спланирована путем подготовки целевых программ, носящих межотраслевой, межведомственный и межрегиональный характер.

Необходимо повысить роль субъектов предупредительной деятельности, где должна быть хорошо отработанной координация и взаимодействие между правоохранительными органами; уточнены функциональные полномочия органов, обеспечено высокопрофессиональное решение поставленных задач через продуманную систему подготовки, переподготовки и повышения квалификации кадров, бережного отношения к специалистам и накопленному опыту.

7.2. Особенности предупреждения преступлений, совершаемых в условиях цифровой трансформации

В условиях развития цифрового общества и внедрения цифровых технологий общество столкнулось с рядом новых негативных социальных явлений, одним из которых является цифровая преступность. Этот вид преступности требует к себе особого внимания и особого подхода в деятельности по ее предупреждению, поскольку еще не выработаны достаточные эффективные механизмы выявления и пресечения преступлений, совершенных в сфере цифровых технологий.

Предупреждение цифровой преступности должно осуществляться на основе коренных изменений стратеги и тактики ее проведения, на поиске и внедрении более эффективных форм и методов проведения квалифицированной работы, которые и должны определить успех предупредительной деятельности в цифровой сфере. Эта деятельность, помимо определения ее целей и задач, а также субъектов системы профилактики, включает информационно-аналитическое обеспечение, криминологическое программирование и планирование профилактических мероприятий, расстановку имеющихся сил и средств, обеспечение их взаимодействия, координацию работы, контроль за исполнением, методическое, кадровое, материально-техническое и иное обеспечение[103].

Эффективность предупреждения преступлений в сфере цифровых технологий зависит, прежде всего, от основ ее организации, которая включает деятельность по формированию самой системы предупреждения преступлений и обеспечению процесса ее функционирования. Она может быть успешной только при комплексном воздействии на причины и условия, способствующие совершению цифровой преступности. С этим нельзя не согласиться, так как преступность – явление, обладающее разноуровневыми характеристиками и детерминированная факторами социального, социально-психологического и индивидуально-психологического порядка, требующее для своего изучения использование комплексного подхода.

Комплексный подход к воздействию на причинный комплекс цифровой преступности обеспечит достижение ощутимого предупредительного эффекта при условии проведения целой системы мер, рассчитанных на длительный период, учитывающих особенности криминологической обстановки.

---

[103] Организация деятельности органов внутренних дел по предупреждению преступлений / под ред. В. Д. Малкова, А. Ф. Токарева. Москва, 2000.

Совокупность наиболее существенных конкретных требований, соблюдение которых в различном сочетании может обеспечить комплексный подход к предупреждению названного вида преступности, характеризуется сочетанием: общесоциального и специального предупреждения; мер общей и индивидуальной профилактики, охватом всех основных сфер жизнедеятельности и институтов социализации гражданина, использованием взаимосвязанных и взаимообусловленных мер экономического, идеологического, культурного, правового, организационно-управленческого характера, взаимодействием и координацией деятельности всех субъектов профилактики, охватом совокупности объектов, требующих профилактического воздействия на совокупность причин и условий, способствующих совершению цифровых преступлений.

Обеспечение комплексного подхода в предупредительной деятельности зависит от выбора направлений и мер предупредительного воздействия. К таковым можно отнести:

– вовлечение всей системы субъектов предупреждения преступности и средств, направленных на снижение негативных явлений, влияющих на рост цифровой преступности;

– взаимодействие и активизация государственных и общественных органов и организаций в сфере предупреждения цифровой преступности;

– использование форм и методов предупреждения цифровой преступности, основанных на результатах научных исследований и внедренных в практическую деятельность правоохранительных органов;

– разработка и реализация федеральных и региональных программ предупреждения цифровой преступности. В современных условиях необходима подготовка теоретически обоснованной и финансируемой программы противодействия цифровой преступности, которая была бы сориентирована на устранение всего комплекса факторов, приводящих к разрастанию и укреплению цифровой преступности. При этом ее подготовка должна строиться на основе «строго выверенных научных данных, к разработке которых следует привлечь квалифицированных сотрудников научных и учебных центров страны, опытных практиков-специалистов, представляющих различные отрасли знании – экономику, право, управление, социологию и др.[104] Только в этом случае программа может быть максимально работоспособной. Здесь же следует отме-

[104] *Пинкевич Т. В.* Криминологические и уголовно-правовые основы борьбы с экономической преступностью: дис. ... д-ра юрид. наук. Москва. 2002.

тить, что в ч. 1 ст. 29 «Функционирование системы профилактики правонарушений» федерального закона «Об основах системы профилактики правонарушений в Российской Федерации» закреплено, что она осуществляется на основе государственных программ Российской Федерации, государственных программ субъектов Российской Федерации, муниципальных программ в сфере профилактики правонарушений;

– необходима подготовка долгосрочной государственной комплексной целевой программы по предупреждению цифровой преступности. Ее основой должна стать ориентация на устранение всего комплекса причин, способствующих совершению преступлений в сфере цифровых технологий.

Подготовка таких программ должна осуществляться с учетом:

– результатов проведенного мониторинга состояния защищенности населения;

– определения степени его криминологической безопасности, выступающей составной частью общей системы национальной безопасности России;

– изучения и определения криминологических угроз и рисков, которые позволят определить «как будет меняться структура преступности, какие будут появляться новые формы организации преступных сообществ, как изменяется преступное поведение под воздействием технологий новой технологической революции и т. п.»[105]. Более того, основой такой работы должны стать результаты работы с использованием методов и программ искусственного интеллекта и анализа больших данных.

Такая подготовка должна вестись совершенно на новом уровне, строго выверенных научных данных, к разработке которых следует привлечь квалифицированных сотрудников научных центров страны в сфере IT – технологий, ученых, представляющих различные отрасли знаний – экономики, право, управление, социологию, практических работников и др.;

– привлечение современных специалистов, имеющих определенные знания в названной сфере. Но самое главное необходима подготовка организационных антикриминальных инструментов, в их числе:

а) разработка новой системы профессионального образовательного процесса, направленного на обучение будущих специалистов правоохранительной деятельности и повышение квалификации

[105] *Овчинский В. С.* Как изучать организованную преступность в XXI веке [Электронный ресурс]. URL: https://izborsk-club.ru/15222 (дата обращения: 30.01.2021).

действующего правоохранительного сообщества способам, методам, приемам и формам выявления, раскрытия и расследования преступлений, совершаемых в сфере цифровых технологий;

б) внесение изменений в учебные программы подготовки и повышения квалификации сотрудников правоохранительных органов;

в) разработка методических рекомендаций по противодействию современным вызовам преступности;

г) техническая оснащенность правоохранительных органов новейшими технологиями цифрового мира;

– учитывая предшествующий опыт, когда граждане, да и юридические лица, не имея достаточных знаний в той или иной сфере, теряли свою собственность, становились банкротами и т. д., созрела необходимость правовой пропаганды и обучения граждан правовым основам цифрового права.

В период подготовки мер по предупреждению цифровой преступности, подготовки программ предупреждения этого вида преступности, необходимо понимать, что цифровая экономика отличается от реальной тем, что она существует только в виртуальном мире и преступления, которые следует предупреждать, тоже совершаются в виртуальном мире.

При мероприятиях по предупреждению цифровой преступности необходимо проводить мониторинг с целью получения сведений об уровне электронной торговли, о количестве интернет-магазинов, осуществляющих электронную торговлю, оборот электронной торговли, количество пользователей компьютерами и имеющих доступ к сети Интернет, уровень компьютерных навыков населения; объем инвестиций в телекоммуникации и др. С целью прогнозирования цифровой преступности особое внимание следует уделять электронному маркетингу, электронному банкингу и электронным страховым услугам.

Субъектами предупреждения цифровой преступности являются федеральные органы государственной власти, органы государственной власти субъектов Российской Федерации, органы местного самоуправления, действующие в пределах своей компетенции как непосредственно, так и через подведомственные им структуры. В предупреждении данного вида преступлений важная роль принадлежит различным государственным и негосударственным структурам, выполняющим функции по обеспечению цифровой безопасности. Ряд таких структур создан законодательными актами, принятыми в Российской Федерации в последние годы.

Участвовать в профилактике могут как отдельные лица, так и общественные объединения и иные организации, которые целенаправленно осуществляют на различных уровнях и в различных масштабах профилактическую деятельность, наделенные, в связи с этим определенными правами и обязанностями и несут ответственность за их реализацию в рамках ч. 1, 7, ст. 10, ст. 13, ч. 1 ст. 17 названного законодательного акта.

В настоящее время в ряде субъектов Российской Федерации работают, например, кибердружины, которые осуществляют мониторинг информационно-телекоммуникационной сети «Интернет» и при обнаружении распространения негативного контента, жестких видеозаписей и картинок, информации нацистского и фашистского содержания, фишинговые рассылки и пр., передают информацию в правоохранительные органы.

Большое значение в предупредительной деятельности играет информационное обеспечение правоохранительных органов. В настоящее время существует недостаточная осведомленность о реальном состоянии и структуре преступлений, совершаемых в сфере цифровых технологий.

В связи с этим необходима разработка и внедрение специальной образовательной программы, предназначенной для обучения будущих специалистов правоохранительной деятельности и повышения квалификации действующего правоохранительного сообщества способам, методам, приемам и формам обеспечения криминологической защиты населения от преступных посягательств; и в тоже время такое же направление деятельности должно быть направлено на обучение населения самостоятельным способам, методам, приемам и формам защиты от преступных посягательств в сфере цифровых технологий.

Однако анализ результатов нашего исследования свидетельствует о том, что при получении информации сотрудники правоохранительных органов сталкиваются со сложностями организационного порядка. Так, например, получение полной информации о преступлениях, совершаемых с использованием цифровых технологий на территории России практически невозможно, так как такая информация разрознена и при ее сборе она не соответствует имеющимся общим показателям отчетности Министерства внутренних дел Российской Федерации. Причина заключается в том, как уже ранее упоминалось, что произошли изменения преступности, появились новые виды, способы и средства совершения преступлений, которые еще не изучены, это, во-первых, а во-вторых, преступления стали совершаться в виртуальной среде, что осложня-

ет их выявление, раскрытие и привлечение виновных к уголовной ответственности.

Такое положение влечет целый ряд негативных последствий, так как органы внутренних дел и другие правоохранительные органы, не имея четкого представления о действительных тенденциях этих преступлений, не располагают достоверными данными о наносимом ими ущербе и, в конечном счете, не имеют достаточной базы для определения необходимого объема мер предупредительного характера.

Большую роль в предупредительной деятельности играет соответствующая правовая база, которая находится только в стадии становления.

Контрольные вопросы

1. Раскройте понятие «предупреждение преступлений».
2. Назовите общесоциальные меры предупреждения преступлений, совершаемых в сфере цифровых технологий.
3. Определите предупредительные меры социально-криминологического характера преступлений, совершаемых в сфере цифровых технологий.
4. Назовите особенности предупреждения преступлений, совершаемых в сфере цифровых технологий.

Глава 8. Виктимологическая профилактика преступлений в сфере развития и использования цифровых технологий

Планируемые результаты освоения темы главы

– **знать** понятия «кибервиктимность» и «кибервиктимизация», сущность виктимологической профилактки, меры виктимологической профилактки;

– **уметь** составлять программы виктимологической профилактки кибервиктимности; применять полученые знания в практической деятельности;

– **владеть** терминологией виктимологии; навыками для организации и проведения виктимологической профилактки.

8.1. Кибервиктимность: понятие и виды

Сегодня жертвами киберпреступников становятся не только люди, но и целые государства. При этом безопасность тысячей граждан – пользователей электронного мира может оказаться под угрозой всего от действий нескольких преступников. В 2007 году была зафиксирована миллионная жалоба на интернет-преступление. Рост профессионализма киберпреступников, совершенствование информационно-коммуникационных технологий приводит к созданию новых угроз для граждан – пользователей электронного мира.

Определение цифровой преступности было дано ранее, отметим, что термины «цифровая преступность» или «киберпреступность» преимущественно зависит от цели использования указанных терминов. Для целей настоящего параграфа определим, что киберпреступность это негативное социальное явление, характеризующееся совокупностью противоправных деяний – цифровых преступлений, совершенных на определенной территории и за определенный временной промежуток.

Термин «киберпреступность» включает в себя большое разнообразие преступлений, что усложняет разработку ее типологии или классификации. Конвенция о киберпреступности[106] группирует их в 4 блока преступлений: против конфиденциальности, целостности

[106] Конвенция о преступности в сфере компьютерной информации (ETS № 185). Заключена в г. Будапеште 23 ноября 2001 г. Доступ из информационно-правового портала «Гарант».

и доступности компьютерных данных и систем; связанными с компьютерами; с контентом; с правами собственности.

Противодействие киберпреступности требует всестороннего подхода, включающего в том числе и активизацию возможностей виктимологической профилактики, которая направлена увеличение защитного потенциала граждан, в нашем случае – участников «цифровых правоотношений» и уменьшение их степени виктимности.

Не вдаваясь в теоретический анализ различных точек зрения по вопросу сущности понятия виктимности, определим, что с одной стороны, виктимность можно рассматривать в ее субъективном аспекте, т. е. в связи с предрасположенностью самого лица стать при определенных условиях жертвой преступления, а, с другой стороны, как повышенную вероятность стать жертвой преступления от состояния самой преступности.

Например, виктимологией установлено, что несовершеннолетние, женщины и физически слабые люди более уязвимы в криминальных ситуациях насильственного характера, или в нашем случае доверчивые, легкомысленные, не обладающие достаточными знаниями люди – для киберпреступлений.

Определим, что «кибервиктимность» – это свойство, потенциально повышающее вероятность возможного становления человека жертвой цифрового преступления, обусловленное совокупностью внешних и внутренних детерминант субъективно-объективного характера.

Внешние – это действия преступного поведения.

Внутренние, относящиеся к потенциальной жертве – гражданину. Характерной особенностью данного вида виктимности являются субъективные свойства человека – легкомыслие, доверчивость, информационная недостаточность необходимых знаний, а к объективным необходимо отнести наличие телекоммуникационных или компьютерных устройств.

Определим, что жертва цифрового преступления – это физическое лицо, являющееся субъектом правоотношений в сфере телекоммуникационных и компьютерных технологий, которому в результате совершения преступления причиняется вред.

Изучение жертв преступных деяний, связанных с использованием телекоммуникационных и компьютерных технологий имеет прикладное значение в связи с ее участием при возникновении виктимной ситуации и, соответственно, возможностью ее предотвращения. Определенные взаимоотношения возникают между преступником и его жертвой при использовании телекоммуникационных и компьютерных технологий, что определяет свою специфику. Если рассматривать в качестве жертвы человека, то киберпреступлением

ему возможно причинить вред только имущественного и морального характера.

Изучение жертвы цифрового преступления необходимо прежде всего в профилактических целях, а точнее, в целях предупреждения новых цифровых преступлений. Такая же задача стоит перед учеными, исследующими жертву преступных посягательств с использованием телекоммуникационных и компьютерных технологий.

Применительно к индивидуальному проявлению кибервиктимности можно говорить о «виктимном поступке», который отражает единичный факт проявления кибервиктимности. Под кибервиктимным поступком следует понимать действие или бездействие, имеющее признаки косвенного умысла или неосторожности в виде легкомыслия или небрежности, способствующее совершению цифрового преступления в отношении лица.

В большинстве случаев жертвы цифрового преступления обладают сходными морально-психологическими и социальными качествами, определяющими ту или иную степень уязвимости от киберпреступлений. Они составляют массу, в которой отдельное лицо с его индивидуальной виктимной предрасположенностью выступает как элемент совокупности (массовая кибервиктимность), которая обладает количественными и качественными свойствами. Поскольку массовая кибервиктимность объективно существующая реальность, то существует возможность определить ее состояние и структуру путем анализа совокупности пострадавших от цифровых преступлений.

Трудно измерить число цифровых преступлений, поскольку их жертвы не всегда сообщают о совершенных в отношении них преступных деяний, а иногда они даже не знают, что в отношении них было совершено преступление. Так, исследования мировой цифровой преступности указывают, что правоохранительные органы получают сообщения о виктимизацйии в результате цифровых преступлений в одном или чуть более проценте случаев. 80 % лиц, ставшие жертвами цифровых преступлений, не сообщили в полицию о факте преступления. Это объясняется и отсутствием общественного доверия к способности полиции бороться с цифровой преступностью и тем, что пострадавшие не знают о механизме сообщения информации, испытывают стыд или неловкость, боятся потери репутации, и т. д. Большинство жертв не осознают, что они стали объектом цифрового преступления, или считают, что причиненный ущерб недостаточно значителен, чтобы обращать на него внимание.

Кроме того, официальная статистика не ведет учет потерпевших от конкретных составов преступлений с использованием телекоммуникационных и компьютерных технологий. Тем не менее,

виктимологические исследования могут помочь в понимании явления – цифровая преступность. Более важно, что точное число цифровых преступлений в каждый отдельно взятый год – тенденция, которую можно определить путем сравнения результатов за последние несколько лет.

Так, подсчет среднеарефмитических показателей преступлений, совершенных с использованием телекоммуникационных и компьютерных технологий за последние три года, позволяет определить доли наиболее виктимных групп граждан, в зависимости от совершенного деяния.

Граждане чаще становятся жертвами следующих видов цифровых преступлений:

1) мошенничество с использованием телекоммуникационных и компьютерных технологий;

2) кражи с использованием телекоммуникационных и компьютерных технологий;

3) мошенничество в сфере компьютерной информации.

Указанные данные соотносятся и с исследованиями цифровой преступности в масштабах всего мира. Указывается, что наблюдается широкий диапазон видов цифровых преступлений. По оценкам правоохранительных структур различных государств преступления, совершаемые в целях получения финансовой выгоды, такие как компьютерное мошенничество или подлог, составляют около одной трети от деяний, совершаемых практически во всех регионах мира. В особенности жертвами указанной формы преступной деятельности становятся граждане–участники электронной торговли и оплаты, электронных аукционах («ebav»), пользователи электронной почты и вебсайтов социальных сетей.

В ряде регионов от одной трети до половины деяний связаны с содержанием компьютерных данных, включая детскую порнографию, контент, связанный с террористическими преступлениями и нарушением прав интеллектуальной собственности. Преступления, связанные с детской порнографией, встречаются чаще в странах Европы и Америки, чем в государствах Азии и Океании или Африки, хотя это может быть связано, скорее, с различиями в приоритетах правоохранительных органов разных регионов, чем с существенными отличиями в составе преступлений. С другой стороны, деяния, совершенные с помощью компьютера и направленные в широком смысле на «причинение личного вреда», более характерны для стран Африки, Америки, Азии и Океании, чем Европы.

По оценкам специалистов, свыше 80 % цифровых преступлений совершаются в той или иной организационных формах, включая форми-

рование единого «теневого рынка» цифровой преступности, основанного на постоянной разработке вредоносного программного обеспечения, заражения пользовательских компьютеров, управления бот-сетями, сбора данных личного и финансового характера, продажи похищенных данных. В связи с существованием указанного преступного сегмента подсчитать точное количество преступных цифровых деяний, а тем более количество пострадавших от них невозможно. Так, отметим, что пострадавшими лишь только от некоторых преступных деяний могу быть сотни или тысячи человек (ст. 273 УК РФ – создание, использование и распространение вредоносных компьютерных программ).

В настоящее время «кибертеневой рынок» характеризуется появлением целых молодежных субкультур, которые занимаются финансовым кибермошенничеством. Данные субкультуры привлекают значительное внимание несовершеннолетних, которые с позднего подросткового возраста становятся жертвами указанного явления, пополняя ряды киберпреступников.

Таким образом, можно говорить о двух значительных группах жертв киберпреступности: потерпевшие от киберпреступлений и жертвы самой киберпреступности, которые под ее влиянием пополняют число киберпреступников.

Виктимизация от цифровой преступности обладает сложной и специфической характеристикой, отличающейся значительным уровнем по сравнению с «обычными» формами преступности. Показатели виктимизации от мошенничества с кредитными картами в режиме онлайн, кражи персональных данных, ответов на попытку фишинга и несанкционированного доступа к учетным записям электронной почты составляют от 1 до 17 процентов. Отметим, что удаленные по решению судов интернет-контенты содержали детскую порнографию, высказывания на почве ненависти, а также диффамацию и критику правительства. Это говорит о значительной степени виктимизации не только граждан, но и самого государства.

По некоторым оценкам, почти 24 % от общего объема глобального потока данных в Интернете представляют собой нарушение авторских прав.

Кибервиктимность на массовом уровне – такое же объективно закономерное явление, как цифровая преступность, а на уровне индивидуальном – всего лишь потенциальная или реализованная предрасположенность конкретного индивида при определенных обстоятельствах становиться жертвой отдельно взятого цифрового преступления. Как мы уже отмечали, конкретное лицо может оказаться жертвой цифрового преступления в силу определенных обстоятельств, а может и избежать такового результата из-за того,

что преступление было начато, но не доведено до завершения в силу определенных обстоятельств как зависящих от потенциального потерпевшего, так и не зависящих от него. Виктимность на индивидуальном уровне может проявиться и может не проявиться в зависимости от обстоятельств конкретного преступления и определенного поведения участвующих в нем сторон – преступника и потерпевшего. Однако при рассмотрении данных закономерностей (состоявшихся или не состоявшихся актов виктимности) на массовом уровне в их совокупности виктимность всегда предстает как реализованная объективная реальность.

Показатели кибервиктимности на массовом уровне значительно *выше*, чем в случае «обычных» форм преступности с учетом соответствующих групп населения, подвергающихся риску. Например, показатели виктимизации от цифровых преступлений варьируются между 1 и 17 процентами населения, имеющего доступ к Интернету, по четырем конкретным деяниям: мошенничество с кредитными картами в режиме онлайн, кража персональных данных, ответы на попытку фишинга и несанкционированный доступ к учетным записям электронной почты, тогда как показатели виктимизации от «обычных» преступлений, таких как кража со взломом, грабеж и кража автомобиля, варьируются от 0,1 до 13 процентов, при этом подавляющее большинство показателей по этим преступлениям не превышает четырех процентов. Одним из факторов, обусловливающих эту разницу, является, по-видимому, «массовый» характер многочисленных цифровых преступлений. В случае таких деяний, как фишинг или взлом пароля электронной почты методом тотального перебора для получения незаконного доступа, отдельный человек может одновременно атаковать большое количество жертв, что невозможно при совершении обычных преступлений.

Реализованная кибервиктимность на массовом уровне влечет серьезные финансовые последствия, включая как прямые, так и косвенные издержки. К таким прямым и косвенным издержкам относятся изъятые со счетов жертв деньги, время и трудозатраты на восстановление данных учетной записи либо ремонт компьютерных систем, а также вторичные затраты, такие как превышение остатка на счете. Косвенные издержки являются денежным эквивалентом потерь, понесенных обществом в результате существования (в целом) самого явления цифровой преступности. Косвенные издержки включают утрату доверия к банковскому обслуживанию через Интернет и падение спроса со стороны частных лиц на услуги электронной системы обслуживания. Совокупные затраты общества вследствие цифровой преступности могут также включать «расходы на защиту», связанные

с приобретением продуктов и услуг, обеспечивающих кибербезопасность, а также расходы на деятельность по обнаружению мошенничества и работу правоохранительных органов.

Разновидностью массовой и индивидуальной кибервиктимности являемся видовая кибервиктимность, которая выражается в относительной «предрасположенности» отдельных людей становиться в силу ряда обстоятельств жертвами определенных видов цифровых преступлений, к примеру, потерпевшими главным образом от краж, с использованием телекоммуникационных и компьютерных технологий или преступлений экстремистской, террористической направленности совершенных с использованием сети Интернет.

Видовая кибервиктимность позволяет наиболее полно выделить основные типичные черты потерпевших от определенной группы цифровых преступлений и осуществить типологию жертв данных преступлений.

Групповая виктимность – разновидность массовой виктимности, которая характерна для определенных групп населения, выделяемых по половому, профессиональному, социальному или иному признаку, и заключается в общей для отдельных категорий людей, обладающих сходными социальными, демографическими, психологическими, биофизическими либо другими качествами, повышающих риск при определенных условиях становиться жертвами преступлений. Например, жители Центрального и Приволжского федеральных округов чаще становятся жертвами цифровых преступлений.

Характеристика кибервиктимности была бы неполной без рассмотрения вопроса о ее латентности, которая наряду с другими причинами и условиями, она обеспечивает существование цифро-

вой преступности. Латентная кибервиктимность – виктимность, не получившая по тем или иным причинам очевидного характера, оставшаяся вне официального учета.

Очевидно, что латентную кибервиктимность, так же как и цифровую преступность вообще, нельзя измерить с исчерпывающей точностью и представить в строго фиксированных количественных показателях. Речь может идти лишь об оценочных суждениях, приблизительных расчетах с немалыми допусками и оговорками, о выводах, основанных зачастую на косвенных данных. Поэтому возможен большой разброс мнений относительно уровня латентности цифровой преступности вообще, и в частности кибервиктимизации. По одним экспертным оценкам соотношение выявленных, зарегистрированных фактов преступлений, а также, соответственно, фактов установления потерпевших от этих преступлений, и их латентность, т. е. не выявление подобных фактов, варьируется в пределах от 1:3 до 1:5; по другим – в соотношении 1:100 и даже большем.

Более точные сведения о латентной кибервиктимности можно получить при рассмотрении этого явления не в целом, а по отдельным видам и группам цифровых преступлений. Поэтому говорить о реальном состоянии кибервиктимности сложно. Мы можем, в силу обозначенных факторов, лишь условно допускать то, что состояние цифровой преступности и кибервиктимности гораздо значительнее и эти явления представляют еще большую распространенность чем это видно из уголовной статистики. Так, в 2015 году статистикой было зарегистрировано 2 382 преступления в сфере компьютерной информации, тогда как «Лаборатория Касперского» зафиксировала 291 млн. фактов противоправных действий, которые могли бы быть квалифицированы по ст.ст. 272 и 273 УК РФ[107].

В завершение представляется возможным определить криминальную кибервиктимность как обусловленное наличием цифровой преступности, массовое, исторически изменчивое системное и социальное явление, проявляющееся в совокупности конкретных деяний (выразившихся в действии или бездействии) или определенных виктимных поступков и лиц, их совершивших, на определенной территории (государство, регион, населенный пункт) за определенный период времени.

[107] *Чекунов И. Г., Шумов Р. Н.* Современное состояние киберпреступности в Российской Федерации // Российский следователь. 2016. № 10.

8.2. Виктимологическая профилактика цифровых преступлений

Поведение жертвы является составным элементом механизма преступления, поэтому одним из необходимых условий повышения эффективности предупреждения цифровых преступлений в рассматриваемой сфере являются меры виктимологической профилактики, направленной на потенциальных жертв данного вида преступлений.

Основой данной деятельности является воздействие на виктимологические факторы, влияющие на совершение преступлений в сфере цифровых технологий. При этом следует учитывать как факт виктимности самих пользователей, так и компьютерных технологий и самих компьютеров как хранилищ информации. Поэтому к разработке мер виктимологической профилактики мошенничества в названной сфере должны привлекаться не только криминологи, но и технические специалисты.

Содержание виктимологической профилактики обусловлено несколькими аспектами. В организационном отношении виктимологическая профилактика имеет особенности, связанные со специальной подготовкой сотрудников правоохранительных органов. Недостаточность профессиональных знаний и практических умений не позволяют им своевременно осуществлять предупредительные мероприятия. Это обусловлено отсутствием в настоящее время приемлемых методических рекомендаций по организации и тактике виктимологической профилактики высокотехнологичных преступлений, конкретных методик работы с жертвами подобных преступлений.

Определенные трудности вызывает также проблема информационного обеспечения виктимологической профилактики цифровой преступности. Поэтому совместная работа правоохранительных органов со службами компьютерной безопасности, изготовителями антивирусных программных продуктов является залогом успеха виктимологической профилактики.

В качестве субъектов осуществления виктимологической профилактики преступности в сфере цифровых технологий выступают как государство в лице правоохранительных органов, так и общественные формирования и иные негосударственные структуры. По своему объему виктимологическая профилактика данного вида преступлений охватывает различные формы поведения, являющиеся закономерным результатом разных вариантов виктимности: легкомысленность поведения, излишнее любопытство, пользователь-

ская небрежность, незнание элементарных мер защиты, возрастные и интеллектуальные особенности и др. В качестве механизма регулирования виктимологической защиты выступают не только нормы права, но и морали, корпоративные и этические правила поведения. В целом виктимологическая профилактика должна быть ориентирована на широкую социальную превенцию в целях минимизации высокотехнологичной преступности как общественно опасного явления.

Виктимологическая профилактика в глобальной сети Интернет осуществляется по следующим основным направлениям:

а) повышение эффективности информационной безопасности, совершенствование программно-технических средств защиты компьютерной информации;

б) противодействие распространению спама по электронной почте;

в) предотвращение использования Интернет в качестве информационного ресурса для предупреждения цифровых перступлений в Интернете. Для этого необходимо создать централизованный информационный ресурс об этих преступлениях в глобальной сети Интернет, обладающий государственной поддержкой и обратной связью с правоохранительными органами.

В зависимости от перспективы необходимо все приведенные меры разделить на два этапа: текущий и последующий.

Для сокращения преступлений, совершаемых в сфере цифровых технологий на текущем этапе необходимо одновременно оказывать воздействие в трех направлениях:

– борьба с анонимностью интернет-пользователей в местах коллективного доступа, владельцев электронных почтовых ящиков, владельцев счетов электронных платежных систем;

– организация полноценного взаимодействия правоохранительных органов, негосударственных субъектов предупреждения и граждан в целях реализации положений виктимологической профилактики;

– правовое регулирование экономических отношений в глобальной сети Интернет, что позволяет устранить экономическую основу этого вида преступлений: вопросы электронной формы сделки по гражданскому законодательству, вопросы регулирования деятельности и ответственности ЭПС, интернет-аукционов, участников дистанционной торговли.

В большей степени жертва цифровых преступлений характеризуется виновной виктимностью, т. е. проявляет неосмотрительность, легкомысленна, неосторожна (выражается это к примеру

в неиспользовании конфиденциальных настроек социальных сетях, принятием запросов о добавлении в друзья от незнакомых людей, переходом в электронной почте попотенциально опасным ссылкам в подозрительных сообщениях и т. д.).

В качестве основной причины такой виктимности можно обозначить отсутствие у большинства граждан навыков использования телекоммуникационных и компьютерных технологий, низкую осведомленность о способах хищения в цифровом пространстве и способах защиты, или легкомысленного отношения к средствам защиты. Из этого следует, что поведение жертвы во многих случаях порождает возможность преступного посягательства.

Основное значение приобретает профилактическая работа органов внутренних дел в отношении граждан, участников цифровых правоотношений. Так органы внутренних дел обязаны выявлять лиц, пострадавших от правонарушений или подверженных риску стать таковыми и проводить с ними профилактическую работу в формах[108]: правового просвещения и правового информирования. Так, например, такое информирование может содержать следующие рекомендации.

1. Визуальная оценка. В данном случае рекомендации могут состоять в следующем: уделять внешнему оформлению интернет-магазина. Имеется в виду прежде всего дизайн сайта. Не стоит принимать в качестве достоверных отзывы пользователей, размещенные на этом же сайте. Правильным решением в данном случае является попытка поиска отзывов на других сайтах. Необходимо обращать внимание на то какую площадь веб-страницы занимает баннерная реклама. Положительную оценку получают сайты, не имеющие ни одной рекламной площадки или имеющие рекламу своих дочерних или наоборот головных предприятий. Отсутствие рекламы – дополнительные удобства для пользователя. Присутствие рекламы означает, что магазин зарабатывает прибыль не на продаже товаров, а на рекламе.

2. Ценовая политика. Пользователям необходимо понимать, что цена товара определяется конъюнктурой рынка и не может резко отличаться от средней. В Интернете достаточно сервисов, предоставляющих возможность поиска того или иного товара. Они помогут определить среднюю стоимость товара среди множества предложений.

[108] Об основах системы профилактики правонарушений в Российской Федерации: федер. закон от 23 июня 2016 г. № 182-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс». Ст. 6, 17.

3. Условия и права. Обратившись в новый интернет-магазин, особое внимание следует обратить на следующие разделы сайта: «о магазине», «об оплате» и «о доставке». Действующие легально интернет-магазины всегда размещают о себе полную информацию: адрес, телефон, реквизиты юридического лица и расчетного счета. Такие магазины обычно работают по системе «оплата товара после доставки». Во многих случаях мошенники просят сделать предоплату за доставку, причем с использованием электронных платежных систем. Отсутствие информации, запутанная система получения товара, предложение совершить предоплату являются признаками мошеннической схемы.

Для противодействия фишингу сегодня используются различные способы совершенствования программно-технических средств защиты информации: постоянная модернизация антифишинговых и антиспам-фильтров почтовыми службами – с одной стороны, и использование клиентами для хранения конфиденциальной информации и обмена ей достаточно защищенных почтовых служб и ящиков – с другой.

В целях виктимологической профилактики целесообразно рекомендовать пользователям использовать наиболее подходящий, «защищенный» и правильно настроенный веб-браузер, который незамедлительно предупреждает пользователя о возможной опасности. Это касается не только браузеров, но и других используемых программ, например, «электронных кошельков» WebMoney. Кроме того, антивирусные пакеты многих производителей этого программного обеспечения пополнились модулями, защищающими пользователя от фишинга.

Однако, как показывает практика, основная проблема связана с небрежностью в вопросах защиты персональной информации самими пользователями. Поэтому важной задачей правоохранительных органов является информационно-просветительская деятельность среди населения по предотвращению цифровых преступлений. При этом, на наш взгляд, не следует увлекаться доведением до населения конкретных преступных схем, используемых преступниками. Дело в том, что вариативность данных схем очень высока, новые способы обмана жертв появляются регулярно и с завидным постоянством, при этом огромная территория нашей страны способствует возникновению «очаговых» схем, имеющих ограниченное распространение. Поэтому простое информирование населения о новых способах, например, совершения мошенничества может иметь противоположный эффект: наиболее виктимные слои населения (пожи-

лые люди, доверчивые и легкомысленные пользователи и т. д.) подобной информацией скорее всего не заинтересуются, а вот преступники могут взять на вооружение сообразительность своих «коллег».

Основная работа сотрудников правоохранительных органов должна заключаться, прежде всего, в доведении до граждан элементарных правил безопасности, таких как недопустимость:

– загрузки из сети Интернет программных продуктов из непроверенных источников; перехода по рекламным ссылкам в интернете, сулящим бесплатные услуги, различные призы или существенные скидки; просмотр корреспонденции от неизвестных адресатов;

– общения в социальных сетях с незнакомыми пользователями, за которыми могут скрываться мошенники, сектанты, вербовщики в террористические организации;

– покупки SIM-карт с рук или оставление своих паспортных данных сомнительным «конторам»;

– отправки денежных переводов лицам, предлагающим посреднические услуги в разрешении проблем с родственниками, знакомыми, якобы попавшими в беду;

– передаче данных с кредитных или дебетовых карт, пользовательских паролей и кодовых слов, запрашиваемых по телефону или через социальные сети от лица друзей, знакомых, кредитных или иных организаций под различными предлогами;

– указания в своем профиле социальной сети личной информации, в том числе о своем образе жизни, планируемых отъездах и т. п.;

– проведения операций в интернет-банкинге без проверки истинности адреса личного кабинета или при наличии дополнительных, не предусмотренных стандартной процедурой, запросов (защита от «фишинга»);

– непринятия срочных мер по блокированию кредитных или дебетовых карт при получении СМС о несанкционированном списании или переводе средств третьим лицам;

– регистрации в личных кабинетах, на интернет-ресурсах или онлайн-магазинах с простыми паролями, состоящими из нескольких цифр, коротких слов, соседних клавиш на клавиатуре, личных памятных дат, адресов или номеров телефонов;

– записей личных паролей на стикерах, приклеенных к монитору, или в других легкодоступных местах.

Таким образом, виктимологическая профилактика должны быть организована с учетом виктимности различных групп

населения; иметь конкретную направленность на осознание необходимости соблюдения мер предосторожности в информационно-телекоммуникационном пространстве; основываться на доступных для населения или работников – неспециалистов рекомендациях по совершенствованию своей защищенности от кибер-угроз.

Контрольные вопросы

1. Что относится к внутренним детерминантам кибервиктимности?
2. Для чего необходимо знать характеристики потенциальных жертв цифровых преступлений
3. Каких видов цифровых преступлений граждане чаще становятся жертвами?
4. Что является правовой основой осуществления виктимологической профилактики кибервиктимности граждан?

Глава 9. Уголовная политика в сфере обеспечения цифровой безопасности

Планируемые результаты освоения темы главы

– **знать** роль уголовной политики в сфере обеспечения цифровой безопасности; понятие цифровой безопасности; понимать характерные ее особенности;

– **уметь** применять свои знания для понимания закономерностей и тенденций развития уголовной политики в сфере обеспечения цифровой безопасности;

– **владеть** терминологией уголовной политики и цифровой безопасности; навыками для организации и проведения криминологических исследований; прогнозирования уголовной политики в сфере цифровой безопасности.

9.1. Понятие цифровой безопасности как системы общественных отношений и объекта уголовно-правовой правовой охраны

В настоящее время одним из главных стратегических приоритетов России является развитие цифрового общества и внедрение новейших информационно-коммуникационных технологий во все сферы общественной жизни и в деятельность органов государственной власти.

В научной литературе целиком оправданным является тезис, в соответствии с которым стремительное развитие и широкое использование информационно-компьютерных технологий привело к формированию фундаментальной зависимости критических национальных инфраструктур от состояния их защищенности в информационном плане.

Кроме того, в последнее время цифровая информация приобретает новые свойства, определяющие как ее социально-экономическую ценность, так и правовое содержание. В первую очередь в настоящее время цифровая информация осознается как важный экономический ресурс.

В настоящее время использование информационных ресурсов, эффективная организация информационных процессов могут существенно увеличить рентабельность многих видов про-

дуктивной деятельности, способствовать разрешению политических, военно-политических, социально-экономических, культурно-просветительских и социальных проблем.

Также цифровая информация становится экономическим товаром, что стимулирует во всем мире рост нового сегмента национальной экономики – информационных услуг. Как любой товар цифровая информация имеет собственника, который обладает правом распоряжаться цифровой информацией по своему усмотрению, а ее несанкционированное использование влечет за собой материальные, репутационные потери для ее правообладателя, несанкционированные действия с цифровой информацией становятся основанием для наступления ущерба для государства, граждан, субъектов хозяйствования.

При этом в развитых странах цифровая информация превратилась в основной предмет труда. То есть отрасль производства, где физическая работа традиционно преобладала, перешла на информационные рельсы, соответственно цифровая информация становится средством производства, которое также требует соответствующей правовой защиты.

Следует указать и на то, что в последние десятилетия цифровая информация приобретает свойства мощного средства воздействия на общественно-политические, идеологические и социально-экономические процессы, становится своего рода оружием, которое требует создания системы противодействия, защиты информационных ресурсов, принадлежащих государственным органам, составляющим государственную, врачебную, личную тайну[109].

Развитие информационных средств ведет к возможности установления такого тотального контроля над людьми, какого еще не было в истории человечества[110].

В современных условиях цифровая информация становится стратегическим ресурсом, правовая зашита которого диктуется необходимостью дальнейшего развития экономики, формирования гражданского общества, обеспечения безопасности государства и граждан. В связи с этим, информационная безопасность является важнейшей составляющей национальной безопасности в целом,

[109] Информатика для юристов и экономистов / под ред. С. В. Симоновича. Санкт-Петербург: Питер, 2002. С. 20.

[110] *Лисичкин В. А., Вирин М. М.* Формирование информационного общества: проблемы и перспективы: монография. Москва: ИСПИ РАН, 2008. С. 36.

а проблема обеспечения цифровой безопасности является чрезвычайно актуальной[111].

В этой связи актуализируется проблема правового регулирования процессов, в которых цифровая информация начинает выступать как основа общественных отношений, возникающих при реализации информационных потребностей государства, личности и общества, т.е. при создании, получении, обработке, накоплении, хранении, поиске, распространении и потреблении цифровой информации, при создании и использовании информационных систем, информационных технологий и средств цифровой безопасности[112].

В научной литературе понятие «информация» осмысливалось на уровне ее коммуникативного признака, как основная часть процесса коммуникации, например существует мнение, что мысль, рожденная в человеческой голове, еще не является информацией, таковой она становится после того, как лицо поделится этой мыслью с другими[113].

Справедливой является точка зрения, в соответствии с которой информация является сложным явлением, образуемое, с одной стороны, проявлением свойства объектов живой природы (субъектов) отражать в форме психических ощущений движение объектов окружающего мира (содержательная сторона информации, сведения), а с другой – проявлением способности некоторых объектов живой природы передавать с помощью сообщений испытанные ими ощущения (образы) другим объектам живой природы (представительная сторона информации, сообщение)[114].

Приведенные выше определения отражают коммуникативную сущность информации, однако в тоже время указывают на ее основу, т. е. на объект коммуникации, каковым являются сведения, обличенные в форму, дающую возможность их передавать и воспринимать.

---

[111] *Бачило И. Л.* Информационное право: учебник для вузов. Москва: Высшее образование; Юрайт-Издат, 2009. С. 398.

[112] *Снытников А.А., Туманова Л. В.* Обеспечение и защита права на информацию. Москва: Городец-издат, 2001. С. 32.

[113] *Иззатов Т. Ш.* Цифровая информация как объект правового регулирования // «Право и жизнь». 2001. № 42. С. 18.

[114] *Стрельцов А. А.* Содержание понятия «цифровая информация» [Электронный ресурс] // Тезисы доклада на заседании Межведомственного междисциплинарного семинара по научным проблемам цифровой безопасности 13 декабря 2001 г. URL: http://geo.web.ru/db/msg.html?mid=1161721 (дата обращения: 14.07.2020).

С точки зрения современных процессов информатизации понятие «данные» более точно отражает характер объектов информационных отношений, в структуру которого входят и сведения, являющиеся теми или иными фактами, имеющими отношение к различным сферам человеческого бытия.

Особенностью понятия «информация» является его универсальность – оно используется во всех без исключения сферах человеческой деятельности[115], в то же время, определение категории «цифровая информация», прежде всего, зависит от конкретной области знаний, в которой ведется исследование. Исходя из приведенных выше определений, мы можем говорить о том, что с правовой точки зрения цифровая информация – это данные, которые являются объектом коммуникации, и посягательство на информацию следует рассматривать в двух плоскостях: как посягательство непосредственно на информацию и как посягательство на возможности ее беспрепятственной передачи (коммуникации).

Таким образом, по мнению законодателя, информация, являясь средством коммуникации, становится объектом правовой защиты уже в момент ее появления, независимо от того, в какой форме она предоставлена и вне зависимости от ее дальнейшего распространения.

Следует признать, что в принципе любая цифровая информация создается с целью ее распространения и использования, поэтому рассматривать цифровую информацию в отрыве от сложного и разнообразного процесса ее передачи и получения практически невозможно. Иными словами, современные представления о содержании понятия «цифровая информация» также связаны со способностями оперировать сведениями, информация представляет собой сообщение, целью которого является передача сведений и данных, относительно идей, открытий о положении дел где-либо, о состоянии чего-либо.

Данный подход имеет под собой целиком прагматические основания, поскольку цифровая информация в статическом состоянии перестает обладать тем огромным массивом полезных качеств, которыми она наделена, будучи способной к передаче. В таком случае она и превращается в просто сведения или данные, чья ценность состоит лишь в содержании, которое они несут. Поэтому, представляется, что под цифровой информацией следует понимать совокупность сведений и данных, процесс их передачи и получения.

---

[115] *Бекман И Н.* Информатика: курс лекций [Электронный ресурс]. URL: http://profbeckman.narod.ru/InformLekc.files /Inf02.pdfc (дата обращения: 07.11.2020).

С правовой точки зрения цифровая информация представляет собой субстанцию, имеющую способность трансформироваться в фактические социально-правые отношения по поводу обладания, распространения, продажи и передачи сведений, которые подлежат правовой защите и охране.

В данном случае под цифровой безопасностью следует считать деятельность по созданию правовых норм, направленных на защиту информации и информационных прав участников процессов, связанных с обращением информации – государства, личности, предприятий и организаций; защитой следует считать процесс использования данных норм в практическом аспекте правоприменения.

По нашему мнению, рассматривая цифровую безопасность как объект уголовно-правовой охраны, следует указать на то, что она является не только состоянием защищенности, но и системой общественных отношений, которые способствуют возникновению состояния защищенности или безопасности.

При этом следует указать на то, что важным признаком цифровой безопасности является ее динамичность, поскольку она, в широком смысле, представляет собой обеспечение стабильности и развития цифровой сферы, которая постоянно меняется из-за многообразия потребностей участников информационных отношений. В связи с последним заметим, что большинство из приведенных определений хоть и фиксируют важные конститутивные признаки цифровой безопасности, однако рассматривают ее как неизменное явление: «состояние защищенности», «способность защищать», «защищенность» и т. д.

Для конкретизации понятия «цифровая безопасность» принципиальным является определение состояния безопасности как совокупности «условий существования субъекта, способностью субъекта контролировать те или иные условия деятельности, осуществлять мониторинг условий, ... способность субъекта оказывать на них определяющее влияние, решающее воздействие, осуществлять реальное доминирование, фактическое господство, власть над ним»[116].

Данное определение дает основания для предварительного рассмотрения цифровой безопасности именно как определенной

[116] *Иващенко Г. В.* Доктрина цифровой безопасности и методические проблемы теории безопасности: материалы круглого стола «Глобальная информатизация и социально-гуманитарные проблемы человека, культуры, общества», МГУ. Москва, 2000. С. 48–63.

системы общественных отношений, возникающих по поводу создания условий безопасной жизнедеятельности государства, общества и личности в цифровой среде.

Фактически на общественном характере цифровой безопасности стоит и Доктрина цифровой безопасности, указывающая, что «информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности Российской Федерации»[117].

В контексте решения задач правового регулирования «системообразующий фактор жизни» объективно требует защиты, которая осуществляется как в рамках информационного права, так и с помощью различных других конструктивных отраслей права: конституционного, гражданского, банковского, коммерческого и т. д. Соответственно, и уголовно-правовая охрана в цифровой среде обеспечивается с помощью норм, которые направлены на защиту различных субъектов цифровой безопасности, государства, общества, личности, хотя при этом трудно не согласиться с Д. А. Калмыковым, утверждающим, что «принцип баланса интересов личности, общества и государства в цифровой сфере законодательно не определен»[118].

Если в действующем законодательстве действительно не отражен баланс интересов участников информационных отношений, то в научной литературе такой баланс в принципе определен.

По мнению исследователей, интересы общества в цифровой сфере заключаются в обеспечении интересов личности в этой сфере, упрочении демократии, создании правового социального государства, достижении и поддержании общественного согласия, в духовном обновлении России.

Интересы государства в цифровой сфере заключаются в создании условий для гармоничного развития российской цифровой инфраструктуры, для реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности

---

[117] Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления»: федер. закон от 9 февраля 2009 г. № 8-ФЗ (ред. от 07.06.2013) // Собр. законодательства Рос. Федерации. № 7. Ст. 776.

[118] *Калмыков Д. А.* Информационная безопасность: понятие, место в системе уголовного законодательства Российской Федерации, проблемы правовой охраны: дис. ... канд. юрид. наук. Москва, 2005. С. 195.

России, политической, экономической и социальной стабильности, в безусловном обеспечении законности и правопорядка, развитии равноправного и взаимовыгодного международного сотрудничества.

Что касается интересов личности в цифровой сфере, то, по нашему мнению, они заключаются в обеспечении свободного доступа к открытой информации, в том, чтобы данная информация была правдивой, не имела своей целью негативное информационное воздействие на личность, не носила антигуманный, аморальный, экстремистский характер, чтобы личная, конфиденциальная информация граждан была надлежащим образом защищена с использованием норм права, чтобы система юридических норм надежным образом гарантировала прав граждан в цифровой сфере.

Приведенные выше подходы являются основанием для того, чтобы определить цифровую безопасность (в юридическом смысле) как совокупность общественных отношений, которые регулируются системой правовых норм, направленных на обеспечение национальных интересов государства, интересов общества, на обеспечение законных интересов личности и субъектов хозяйствования в цифровой сфере, гарантируют права человека и гражданина в цифровой сфере, защиту информации от несанкционированного доступа, уничтожения, блокирования, модификации, копирования и неправомерного использования.

В рамках первой группы обеспечивается функционирование эффективных средств цифровой деятельности, в рамках второй – обеспечивается возможность субъектов получать доступ к необходимым цифровым ресурсам, формируется цифровой ресурс, отвечающий потребностям субъектов, третья группа обеспечивает функционирование цифровой информации, имеющей режим тайной, конфиденциальной, четвертая группа отношений определяет состояние общественной безопасности, связанной с использованием компьютеров и цифровых технологий.

В процессе исследования проблем цифровой безопасности возникает проблема разграничения данного вида безопасности и безопасности общественной, поскольку, поместив главу 28 УК РФ в раздел IX «Преступления против общественной безопасности и общественного порядка», законодатель определил родовой объект посягательства преступлений в сфере компьютерной информации как отношения общественной безопасности, что представляется достаточно спорным. Отметим, что ученые, исследовавшие проблемы общественной безопасности и общественного порядка, не склон-

ны относить преступления в сфере цифровой безопасности к данному виду преступности[119].

Однако, как указывает К. С. Бельский, общественная безопасность наряду с государственной, экономической, военной, политической, экологической, цифровой является разновидностью национальной безопасности[120]. Таким образом, в данном случае фактически ставится знак равенства между общественной и цифровой безопасностью в смысле их юридической значимости, т. е. цифровая безопасность не рассматривается как элемент общественной безопасности, а получает целиком самостоятельную регламентацию.

Объектом посягательства при совершении преступлений, направленных против общественной безопасности, выступают безопасные условия жизни людей в процессе производства различного рода работ; обращения с источниками повышенной опасности; нормального функционирования государственных и общественных институтов; в сфере социального общения человеческих индивидов, которым причиняется вред в результате совершения преступлений данного вида.

В данном случае речь идет об отношениях по поводу безопасности при использовании источников повышенной опасности на транспорте, на производстве в области экологии, нарушение которых способно причинить общественный вред.

На наш взгляд цифровая безопасность в отдельных случаях обеспечивает безопасные условия при производстве различного рода работ, также посягательство на цифровую безопасность оказывает влияние на безопасные условия жизни общества, однако, по своей юридической сущности данная форма безопасности выходит за рамки производственного аспекта безопасности, сам компью-

---

[119] *Ковалев М. И.* Преступления против общественной безопасности // Уголовное право. Особенная часть: учебник / М. И. Ковалев, В. Н. Петрашев / под ред. проф. В. Н. Петрашева. Москва, 1999; *Боков А. В.* Преступления против общественной безопасности // Уголовное право России. Практический курс: учеб.-практическое пособие; *Комиссаров В. С.* Преступления против общественной безопасности // Уголовное право Российской Федерации. Особенная часть: учебник / под ред. Г. Н. Борзенкова и В. С. Комиссарова. Москва, 2004; *Зелинская Н. А.* Преступления против общественной безопасности // Уголовное право Российской Федерации. Особенная часть: учебник / под ред. проф. Л. В. Иногамовой-Хегай, проф. А. И. Рарога, А. И. Чучаева. Москва, 2004; *Малков В. П.* Преступления против общественной безопасности // Уголовное право России. Часть Особенная: учебник для вузов / отв. ред. Л. Л. Кругликов. 3-е изд., перераб. и доп. Москва, 2005.

[120] *Бельский К. С.* Полицейское право: лекционный курс. Москва: «Дело и Сервис», 2004.

тер едва ли следует рассматривать как источник повышенной опасности, хотя как и каждое преступление, данный вид преступности посягает на безопасные условия общественной жизни.

В свою очередь родовым объектом информационно-правовой защиты в сфере обеспечения общественной безопасности Российской Федерации являются информационные права, свободы и законные интересы граждан, общества и государства, а предметно-отраслевым – правоотношения, возникающие в процессе реализации прав гражданина, общества и государства на получение, хранение, распространение, пользование цифровой информацией, а равно и ее защиты.

В данном случае речь идет о цифровых правоотношениях, которые оказывают воздействие на общественную безопасность и общественный порядок. Примером тесного взаимодействия цифровой и общественной безопасности может служить сокрытие цифровой информации, распространение ложной цифровой информации, что ведет к нарушению общественного порядка, к нарушению функционирования технических, технологических и экологических систем, нарушения функционирования органов государственной власти и местного самоуправления, к проблемам с безопасностью личности в современной техногенной среде.

В соответствии с Федеральным законом от 9 февраля 2009 г. № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления», к основным принципам обеспечения доступа к информации о деятельности государственных органов и органов местного самоуправления относятся: открытость и доступность информации о деятельности государственных органов и органов местного самоуправления; достоверность информации о деятельности государственных органов и органов местного самоуправления и своевременность ее предоставления; свобода поиска, получения, передачи и распространения информации о деятельности государственных органов и органов местного самоуправления любым законным способом; соблюдение прав граждан на неприкосновенность частной жизни, личную и семейную тайну, защиту их чести и деловой репутации, права организаций на защиту их деловой репутации при предоставлении информации о деятельности государственных органов и органов местного самоуправления[121].

[121] Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления: федер. закон от 9 февраля 2009 г. № 8-ФЗ (ред. от 07.06.2013) // Собр. законодательства Рос. Федерации. № 7. Ст. 776.

Часть 5 ст. 29 Конституции Российской Федерации признает свободу массовой информации и запрещает цензуру, что прямым образом связано с правом на доступ к информации, т. к. ее основная масса передается посредством СМИ, к которым, в соответствии с законом «О средствах массовой информации», относятся периодические издания, радио-, теле-, видеопрограммы и иные формы периодического распространения информации.

Взаимодействие и поддержание обратной связи граждан с государственными органами следует считать неотъемлемым звеном права на доступ к информации. Информационные права и свободы граждан находятся в органической связи с обязанностями государства в цифровой сфере.

Ограничение права на доступ к информации в соответствии со ст. 55 Конституции Российской Федерации, может иметь место только «в той мере, в какой это необходимо в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства[122].

В то же время Конституция Российской Федерации в ст.ст. 21, 23, 24, 29, 44, 46 и 56 устанавливает и ряд принципиальных положений, касающихся гарантий цифровой безопасности.

Таким образом, конституционное право на свободу получения цифровой информации является не только основой информационных отношений, но и гарантом прозрачности, а, следовательно, законности деятельности государственной власти. Рассмотренные выше положения Конституции нашли отражение в уголовном праве, например, ст. 140 УК РФ устанавливает ответственность должностных лиц за отказ в предоставлении гражданину информации, а также за предоставление гражданину неполной или заведомо ложной информации.

Данное определение соотносится с положениями Конституции Российской Федерации, в которой в ст. 2 указано, что «Человек, его права и свободы являются высшей ценностью. Признание, соблюдение и защита прав и свобод человека и гражданина – обязанность государства»[123].

Таким образом, можно сказать, что цифровая безопасность представляет собой сложную конституционно-правовую конструкцию, что определяется ее сложной социальной и правовой природой, осно-

---

[122] Конституция Российской Федерации (принята всенародным голосованием 12 декабря 1993 г. с изменениями, одобренными в ходе общероссийского голосования 01.07.2020). Доступ из справ.-правовой системы «КонсультантПлюс».

[123] *Там же.*

ванной на многообразии цифровых отношений в обществе; на дифференциации субъектов цифровых отношений, имеющих свои интересы, права и обязанности в данной сфере; на объективном характере цифровых отношений, которые в начале XXI века определяют развитие мировой цивилизации и системы международного права.

Современный мир невозможно представить без цифровых технологий, которые трансформировали не только принципы и формы сбора, обработки и передачи цифровой информации, они начали осуществлять мощное воздействие на культурный, экономический, политический, военно-стратегический аспекты общественной жизни. Цифровые технологии стали одним из основных факторов обеспечения и поддержания стабильного развития, а количество, технический уровень и доступность цифровых ресурсов определяют уровень развития страны и ее статус в мировом сообществе. В то же время развитие цифровых технологий обусловило не только переход национальных инфраструктур на принципиально новый уровень развития и функционирования, но и привело к возникновению новых угроз системам национальной и международной безопасности и породило целый комплекс негативных последствий.

Эти угрозы связаны, прежде всего, с возможностью использования цифровых технологий в целях, несовместимых с правами и свободами человека, поскольку они нарушают фундаментальные принципы, заложенные еще во Всеобщей декларации прав человека. В частности, речь идет о нарушении принципа уважения достоинства и прав личности (ст. 1), о нарушении права личной неприкосновенности (ст. 3), о нарушении имущественных прав (ст. 17), о нарушении положений ст. 12 данной Декларации, где речь идет о том, что никто не может подвергаться произвольному вмешательству в его личную и семейную жизнь, произвольным посягательствам на неприкосновенность его жилища, тайну его корреспонденции или на его честь и репутацию, а также ст. 19 Декларации в соответствии с которой каждый человек имеет право «искать, получать и распространять информацию и идеи любыми средствами и независимо от государственных границ».

При этом Всеобщая декларация прав человека провозглашает, что все люди равны перед законом и имеют право без всякого различия на равную защиту закона. Каждый человек имеет право на равную защиту от какой бы то ни было дискриминации, нарушающей настоящую Декларацию (ст. 7), при том, что в ч. 2 ст. 27 Декларации указано, что каждый человек имеет право на защиту его моральных и материальных интересов, являющихся результатом научных, литературных или художественных трудов, автором которых он является.

9.2. Уголовная политика Российской Федерации и международная цифровая безопасность

В начале XXI столетия в сфере цифровой безопасности наблюдаются новые негативные тенденции, особую озабоченность вызывает возможность разработки, применения и распространения информационного оружия, возникновение в связи с этим угрозы информационных войн и информационного терроризма, чьи разрушительные последствия можно сравнить с последствиями применения оружия массового уничтожения. В геополитических масштабах цифровые технологии превращаются в важный стимул развития военного потенциала стран за счет повышения их цифровой обеспеченности. В свою очередь, это неизбежно ведет к ускорению поляризации мира, что порождает нестабильность, возникновение и развитие реальных и потенциальных угроз и конфликтов. Именно в связи с этим, как указывает В. И. Степанов-Егиянц, в настоящее время государства включают в свою правовую систему общепризнанные принципы и нормы международного права, а также международные договоры. По этому пути пошла и Российская Федерация, закрепив в ст. 15 Конституции, что общепризнанные принципы и нормы международного права, а также международные договоры России являются составной частью ее правовой системы. Многие ученые считают, что этим положением констатируется, что общепризнанные принципы и нормы международного права в принципе не противоречат Конституции и нормативным Правовым актам, составляющим правовую систему Российской Федерации, и что правоприменители в пределах своей компетенции не только вправе, но и обязаны применять правила международных договоров для разрешения конкретных дел. Кроме того, Конституция РФ идет значительно дальше в признании приоритета международных договоров Российской Федерации перед нормами национального законодательства, поскольку в случае коллизии между ними предпочтение отдается международному договору.

Подобная ситуация характерна и для других стран, из конституций которых и было заимствовано подобное положение. Таким образом, подобное положение международного права в правовой системе заставляет изначально поднимать проблему международно-правового регулирования, а затем уже анализировать конкретные положения национальных законодательств.

Проблематика международной цифровой безопасности выделилась в международном праве в 90-х гг. XX столетия. Этому способствовал ряд факторов, в первую очередь – многообразие негативных

проявлений использования информационно-коммуникационных технологий. Эти новые технологии оказались способными осуществлять негативное влияние как на реализацию основных прав и свобод человека, так и на целостность государственных инфраструктур. Их быстрое и широкомасштабное развитие, разнообразное воздействие на субъектов отношений и растущая зависимость мирового сообщества от надлежащего функционирования информационно-коммуникационных сетей и систем усилила внимание к этим новым проблемам как с практической, так и теоретической точек зрения, и первенство в данном процессе, несомненно, принадлежит Организации Объединенных Наций (далее – ООН).

Нормативно-правовая база, касающаяся проблем цифровой безопасности на международном уровне, начала складываться на протяжении последних тридцати лет, хотя в данном процессе наблюдается отсутствие единомыслия.

Дискуссии по проблеме информационного общества, развернувшиеся в последней четверти прошлого столетия, привели к тому, что в международном праве возникли полярные мнения относительно регулирования общественных отношений, касающихся проблем цифровой безопасности. Можно утверждать, что в международном праве до сих пор не удалось создать единого подхода к определению цифровой безопасности.

Принципиальные разногласия в доктринальных взглядах заключаются в следующем. Сторонники первой концепции, которых поддерживает Россия, базируют свою позицию на широком понимании проблематики международной цифровой безопасности.

Еще в 1998 году по результатам 53-й сессии ГА ООН была разработана резолюция (A/RES/53/70) «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», которая предложила государствам-членам ООН продолжить обсуждение вопросов цифровой безопасности, дать конкретные определения угроз, предложить свои оценки проблемы, включая разработку международных принципов обеспечения безопасности глобальных информационных систем.

Резолюция 53/70 положила начало обсуждению вопросов создания совершенно нового международно-правового режима, субъектом которого в перспективе должны стать цифровая информация и информационная технология.

Согласно ее рекомендациям, Институтом ООН по проблемам разоружения и Департаментом по вопросам разоружения Секретариата ООН в августе 1999 г. в Женеве был организован международный семинар по вопросам информационной безопасности,

в работе которого приняли участие представители более 50 стран наиболее развитых в информационно-технологическом плане.

В целом, можно говорить о том, что в основу этой концепции положены принципы неделимости безопасности и ответственности государств за свое информационное пространство. Ее сторонники, в свою очередь, настаивают на том, что противодействие угрозам военного (военно-политического), террористического и криминального характера с использованием цифровых технологий, должно осуществляться системно. Соответственно, международно-правовое регулирование должно быть распространено на все указанные структурные элементы, и ради достижения этого предложено принятие международного соглашения на универсальном уровне.

По результатам работы 55-й сессии ГА ООН в 2000 г. был одобрен новый проект резолюции (A/RES/55/28), в котором отмечается, что для уменьшения и ограничения угроз в сфере цифровой безопасности необходимо изучение международных концепций, направленных на укрепление безопасности глобальных информационных и телекоммуникационных систем. Такое положение было чрезвычайно важным, поскольку стало основой для следующего этапа решения проблем цифровой безопасности в ООН[124].

Кроме того, в соответствии с рекомендациями резолюции 55/28, был подготовлен проект документа (A/56/164/Add.1) «Общая оценка проблем цифровой безопасности. Угрозы международной цифровой безопасности», в котором выделены и описаны одиннадцать основных факторов, создающих опасность основным интересам личности, общества и государства в информационном пространстве, то есть являются наибольшими угрозами цифровой безопасности[125].

К таким факторам относятся: разработка и использование средств несанкционированного вмешательства в работу цифровых компьютерных технологий, неправомерное использование и нанесение ущерба цифровым ресурсам другого государства; целенаправленное цифровое воздействие на критические инфраструктуры и населения другого государства; действия, направленные на доминирование в цифровом пространстве, поощрение терроризма и ведения информационных войн.

---

[124] Международное сотрудничество в области цифровой безопасности (справочная цифровая цифровая информация) [Электронный ресурс]. URL: http://www.ln.mid.ru/ns-dvbr.nsf/0/4c86fcb9f8dc1b41c3256 e320 029b1ef?OpenDocument (дата обращения: 03.12.2020).

[125] Генеральная Ассамблея Организации Объединенных Наций. Резолюции [Электронный ресурс]. URL: http://www.un.org/ru/ga/sessions.

В резолюции A/RES/56/19, которая была принята в 2001 году, одобрена идея создания в 2004 году специальной Группы правительственных экспертов государств-членов ООН для проведения всестороннего исследования проблемы цифровой безопасности[126]. Прерогативой деятельности этой структуры должно стать рассмотрение существующих и потенциальных угроз в сфере цифровой безопасности и совместных мер по их устранению, а также изучение международных концепций укрепления безопасности глобальных информационных и телекоммуникационных систем.

ГА ООН 22 ноября 2002 г. была принята резолюция по цифровой безопасности (A/RES/57/53), которая развивает положения предыдущих резолюций и указывает на недопустимость использования цифровых технологий и средств с целью оказания негативного воздействия на инфраструктуру государств[127]. Резолюция определяет также направления деятельности ООН.

Основной идеей создания универсального режима цифровой безопасности могло бы стать обязательство участников не прибегать к действиям в информационном пространстве, целью которых является нанесение ущерба цифровым сетям, системам, ресурсам, процессам и инфраструктуре другого государства, подрыв политической, экономической и социальной систем, массированная психологическая обработка населения для дестабилизации общества и государства.

Следующим спорным вопросом является необходимость в международно-правовом регулировании функциональных элементов международной цифровой безопасности. Дело в том, что существуют два основных направления международно-правового регулирования использования цифровых технологий: информационный («содержательный») и коммуникационный («технический»). В доктрине соответствующие информационный и коммуникационный элементы определяются как функциональные.

В международно-правовой проблематике цифровой безопасности они рассматриваются с позиций противодействия использования цифровых технологий, направленного на вред основным правам и свободам человека и критически важным структурам государств. В частности, в случае с информационным («содержательным») направлением это противодействие

[126] Международное сотрудничество в области цифровой безопасности (справочная цифровая информация) [Электронный ресурс]. URL: http://www.ln.mid.ru/ns-dvbr.nsf/0/4c86fcb9f8dc1b41c3256e320029b1ef?Open Document (дата обращения: 01.04.2021).

[127] *Там же.*

трансграничному распространению посредством цифровых технологий информации, что противоречит принципам и нормам международного права, разжигает межнациональную, межрасовую и межконфессиональную вражду, распространяет расистские, ксенофобские письменные материалы, изображения или любую демонстрацию идей или теорий, которые пропагандируют, подстрекают к ненависти, дискриминации или насилию против любой личности или группы лиц. Кроме того, проявления могут выражаться через использование цифровой инфраструктуры для размещения информационных ресурсов, пропагандирующих насильственные действия с целью устрашения, подавления и навязывания определенной линии поведения; распространение призывов к свержению существующего государственного строя и правительства в других государствах, проведение экстремистских и террористических актов; сообщений о совершенных или запланированных актах (в том числе и в информационно-коммуникационных сетях) и т. д. В случае с коммуникационным («техническим») направлением – это противодействие использованию цифровых систем, процессов и ресурсов против коммуникационных сетей и критически важных структур других государств, что наносит ущерб функционированию финансовой, политической, экономической и социальной системам. Эти функциональные элементы (информационный и коммуникационный) тесно связаны со структурными элементами (криминальным, террористическим и военным). Фактически складывается ситуация, когда каждому из структурных элементов соответствует определенный круг разноуровневых функциональных элементов.

Следующий вопрос связан с местом международной цифровой безопасности в системе международной безопасности. Речь идет о признании международной цифровой безопасности в качестве составляющей в системе международной безопасности. Вопрос в основном имеет теоретическую направленность и на начальном этапе был связан с предложенной в 80-х гг. XX ст. концепцией всеобъемлющей системы международной безопасности. Несмотря на то, что концепция создания всеобъемлющей системы международной безопасности представляла собой политическую концепцию достижения безопасности всей межгосударственной системы, в правовой доктрине ее связывали с международным правом. Координирующая роль в процессе обеспечения цифровой безопасности принадлежит ООН, деятельность которой сосредоточена на вопросах, связанных с:

1) борьбой с преступным использованием цифровых технологий[128];

2) международной цифровой безопасностью[129];

3) созданием глобальной культуры цифровой безопасности и защита важнейших информационных структур[130].

Продолжает деятельность Группа правительственных экспертов ООН, созданная с целью исследования существующих и потенциальных угроз в сфере международной цифровой безопасности и возможных совместных мер по их устранению.

Сторонники второй, «узкой» концепции, настаивают на том, что основу международной цифровой безопасности составляет только один элемент – борьба с уголовными преступлениями в сфере цифровых технологий. Именно он, по мнению сторонников, требует международно-правового регулирования. Реализуя данную концепцию в практическом плане, Совет Европы разработал Конвенцию о киберпреступности, которая вступила в силу 1 июля 2004 г.

В рамках этой концепции, в связи с тем, что ее сторонники не рассматривают террористический и военный элементы как составные элементы международной цифровой безопасности, вопрос о регулировании функциональных элементов (информационного и коммуникационного) не рассматривается как перспективный для международно-правового разрешения. Считается, что существующей Конвенции о киберпреступности от 23 ноября 2001 г. и Дополнительного протокола к Конвенции о киберпреступности, который касается криминализации действий расистского и ксенофобского характера, совершенных через компьютерные системы от 28 января 2003 г., в которых совмещены функциональные элементы, достаточно для международно-правового регулирования.

В конце 2005 г. Конвенцию о киберпреступности подписали 38 стран-членов Совета Европы, а также США, Канада, Япония

---

[128] Борьба с преступным использованием информационных технологий [Электронный ресурс]: резолюции Генеральной Ассамблеи Организации Объединенных Наций № 55/63 от 4 декабря 2000 г., № 56/121 от 19 декабря 2001 г. URL: https://ifap.ru/ofdocs/un/56121.pdf

[129] Достижения в сфере информации и коммуникации в контексте международной безопасности [Электронный ресурс]: резолюции Генеральной Ассамблеи Организации Объединенных Наций № 53/70 от 4 декабря 1998 г., № 54/49 от 1 декабря 1999 г., № 55/28 от 20 ноября 2000 г., № 56/19 от 29 ноября 2001 г., №57/53 от 22 ноября 2002 г., № 58/32 от 8 декабря 2003 г., № 59/61 от 3 декабря 2004 г., № 60/45 от 8 декабря 2005 г., № 61/54 от 6 декабря 2006 г., № 62/17 от 5 декабря 2007 г., № 63/37 от 2 декабря 2008 г., № 64/25 от 2 декабря 2009 г., № 65/41 от 8 декабря 2010 г., № 66/24 от 13 декабря 2011 г., № 67/27 от 3 декабря 2012 г.). URL: https://www.un.org/ru/development/ict/res.shtml.

[130] Создание глобальной культуры кибербезопасности и защита важнейших информационных структур [Электронный ресурс]: резолюции Генеральной Ассамблеи Организации Объединенных Наций № 57/239 от 20 декабря 2002 г., № 58/199 от 23 декабря 2003 г., № 64/211 от 21 декабря 2009 г.: URL: https://www.un.org/ru/development/ict/res.shtml.

и ЮАР. Данная конвенция – первый документ, в котором представлена классификация киберпреступлений. В их перечень входят несанкционированный доступ в цифровую среду, нелегальный перехват цифровых ресурсов, вмешательство в цифровую систему и информацию, содержащуюся на носителях данных и т. д. Также в документе описаны проблемы взаимодействия правоохранительных органов в случаях, когда киберпреступник и его жертва находятся в разных странах и подчиняются разным законам. В конвенции освещаются вопросы хранения личной информации клиентов интернет-провайдеров. Россия не подписала механизмы трансграничного доступа к информации, обоснованно считая, что формулировка конвенции наносит ущерб национальной безопасности России в цифровой сфере[131].

Вероятным составным элементом, который имеет определенную перспективу дальнейшего международно-правового регулирования, сторонники этого подхода называют борьбу с терроризмом в цифровой сфере. Возможность международно-правового регулирования использования цифровых технологий в военной сфере не рассматривается как необходимая, поскольку считается, что существующих международно-правовых средств достаточно для регулирования военных конфликтов и войн.

Преступления против цифровой безопасности в том или ином виде включены в уголовное законодательство зарубежных стран. В целом, можно утверждать, что информационная безопасность в ее международно-правовых основах представляет собой широкий перечень документов, который является основой для конструирований аналогичного понятия в российской национальной доктрине цифровой безопасности, а также для ее понимания в уголовно-правовом смысле.

Контрольные вопросы

1. Определите особенности уголовной политики в сфере обеспечения цифровой безопасности.
2. Назовите основные направления уголовной политики в сфере обеспечения цифровой безопасности.
3. Определите роль уголовной политики в сфере обеспечения цифровой безопасности.
4. Назовите документы, регулирующие уголовную политику в сфере обеспечения цифровой безопасности.

[131] Обзор: В. В. Путин отказался подписать Конвенцию о киберпреступниках [Электронный ресурс]. URL: http://virusinfo.info/showthread.php?t=20553 (дата обращения: 16.10.2020).

Глава 10. Международный опыт сотрудничества государств по предупреждению цифровой преступности

Планируемые результаты освоения темы главы

– **знать** основные направления международного сотрудничества государств в сфере предупреждения цифровой преступности;

– **уметь** применять свои знания для понимания закономерностей и тенденций развития цифровой преступности в мире; исследовать вопросы по противодействию цифровой преступности с использованием опыта международных органов и организаций в борьбе с преступлениями, совершаемыми в сфере цифровых технологий (Интерпол, Европол, ФАТФ и др.);

– **владеть** терминологией цифровой преступности; знаниями правовых основ международного сотрудничества в сфере предупреждения цифровой преступности.

10.1. Деятельность ООН по предупреждению цифровой преступности

Международное сотрудничество по предупреждению преступности прошло длительный путь, тем самым заложив международно-правовые основы борьбы с преступностью. Оно реализуется на глобальном, региональном и национальном уровнях и осуществляется на основании международных соглашений и в рамках международных органов и организаций. Реализация международных и национальных многосторонних Конвенций и региональных соглашений составляет основу такого сотрудничества. При этом государства стремятся к объединению усилий в противодействии наиболее опасным преступлениям. К таковым, как показывают результаты исследований последних пяти лет относят и цифровую преступность[132].

В международном сотрудничестве в сфере противодействия цифровой преступности так или иначе участвуют все главные и вспомогательные органы, и организаций ООН, но помимо их роли в противодействие преступности, свою нишу занимают и органы

[132] *Pinkevich, T. V., Rakhmanova, E. N.* Digital Crime Concept Proceedings of the 2nd International Scientific and Practical Conference «Modern Management Trends and the Digital Economy: from Regional Development to Global Economic Growth» MTDE. 2020.

и организации регионального уровня. Все они активно включились в работу по противодействию новым вызовам преступности.

За годы существования ООН создан обширный свод стандартов и норм в области предупреждения преступности и уголовного правосудия, имеющий криминологическое значение. Однако вопросам противодействия цифровой преступности особое внимание стало уделяться только с 2000 г. Так, по итогам работы X Конгресса (Вена, 2000 г.) была принята «Венская декларация о преступности и правосудии: ответы на вызовы XXI века», в рамках которой государства-участники приняли на себя обязательства по укреплению международного сотрудничества и взаимной правовой помощи в целях пресечения ряда преступлений (незаконного оборота оружия, коррупции, экономической преступности, в том числе и легализации преступных доходов, коррупции, терроризма, транснациональной преступности) и противодействия им. В их числе указывалось и предупреждение преступлений, связанных с использованием компьютеров, группа которых сегодня входит в состав цифровой преступности.

В соответствии с итогами Конвенции принимается ряд проектов резолюций Ассамблеи ООН, которые были направленны на укрепление безопасности глобальных информационных и телекоммуникационных систем и общей оценки проблем в названной сфере[133]. Позже еще принимается ряд резолюций Ассамблеи ООН, которая развивает положения предыдущих резолюций[134], в том числе и Соглашения о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации от 1 июня 2001 г.[135]

Позже в Бангкоке в рамках работы XI Конгресс (2005 г.) принимается декларация «Взаимодействие и ответные меры: стратеги-

[133] Международное сотрудничество в области цифровой безопасности (справочная цифровая цифровая информация) [Электронный ресурс]. URL: http://www.ln.mid.ru/ns-dvbr.nsf/0/4c86fcb9f8dc1b41c3256 e320 029b1ef?OpenDocument; Генеральная Ассамблея Организации Объединенных Наций Резолюции. [Электронный ресурс]. URL: http://www.un.org/ru/ga/sessions/.

[134] Международное сотрудничество в области цифровой безопасности (справочная цифровая цифровая информация) [Электронный ресурс]. URL: http://www.ln.mid.ru/ns-dvbr.nsf/0/4c86fcb9f8dc1b41c3256e320029b1ef?OpenDocument; Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации от 1 июня 2001 г. [Электронный ресрс]: ратифицировано Федеральным законом Российской Федерации от 1 октября 2008 г. № 164-ФЗ. URL: http://docs.cntd.ru/document/902140948.

[135] Соглашения между правительствами государств – членов ШОС о сотрудничестве в области обеспечения международной цифровой безопасности от 16 июня 2009 г. [Электронный ресурс]. URL: http://www.worklib. ru/l aw/96355/.

ческие союзы в области предупреждения преступности и уголовного правосудия», в которой особое внимание уделено укреплению международного сотрудничества в противодействии различным формам преступной деятельности, в том числе, киберпреступности, легализации (отмыванию) преступных доходов, терроризму, незаконному обороту культурных ценностей и др. Как видим, с расширением преступной деятельности в киберпространстве, распространением преступных посягательств не только с использованием компьютерных средств, но и в отношении хранящейся в них информации, осознание опасности этих преступлений международному сообществу, способствовало принятию решения на уровне Конгресса ООН о участии в предупреждении киберпреступности мирового сообщества.

В ходе очередного XII Конгресса ООН по предупреждению преступности и уголовному правосудию (12–19 апреля 2010 г.), который состоялся в г. Сальвадоре в Бразилии, с учетом выработанных выводов и рекомендаций[136], одобренных Генеральной Ассамблеей в ее резолюции 62/1734[137], способствовал расширению возможности обсуждения проблем, связанных с противодействием киберпреступности, а также определению современных международных подходов по противодействию не только киберпреступности, но и транснациональной организованной преступности. Особо подчеркнули сложность выявления таких преступлений, их документирование и квалификация[138]. Через три года Управление по наркотикам и преступности ООН подготовило проект исследований в этой сфере, в котором представлено международно-правовое определение киберпреступности (2013 г.), позволившее очертить круг деяний, входящих в эту группу преступлений, раскрыть характеристику личности киберпреступника и особенности деятельности транснациональной организованной преступности в этой сфере.

[136] Доклад совещания Межправительственной группы экспертов по рассмотрению уроков, извлеченных из опыта Конгресса ООН по предупреждению преступности и уголовному правосудию [Электронный ресурс]. Бангкок. 2006. 15–18 августа. URL: https://undocs.org/ru/A/CONF.213/9 (дата обращения: 01.09.2019).

[137] Сальвадорская декларация о комплексных стратегиях для ответа на глобальные вызовы: системы предупреждения преступности и уголовного правосудия и их развитие в изменяющемся мире. Принята резолюцией 65/230 Генеральной Ассамблеи от 21 декабря 2010 г. [Электронный документ]. URL: http://www.un.org/ru/documents/decl_conv/declarations/salvador_declaration.shtml.

[138] XII Конгресс ООН по предупреждению преступности и уголовному правосудию [Электронный ресурс]. Сальвадоре. Бразилия. 12–19 апреля 2010 г. URL: https://undocs.org/ru/A/CONF.213/9 (дата обращения: 05.10.2020).

Позже расширяется понятие киберпреступности и в своем докладе «Предупреждение, защита и международное сотрудничество в области борьбы с использованием новых информационных технологий для надругательства над детьми и (или) их эксплуатации» (2014 г.) Генеральный секретарь ООН дает оценку влияния новых информационно-телекоммуникационных технологий на ситуацию с насилием над детьми и их эксплуатацией[139]. Все больше возникает проблемных вопросов в связи с появлением и распространением нового финансового инструмента, такого как виртуальный актив (криптовалюта).

Вопрос о реагировании на наличие виртуальных активов (криптовалюты) стал все чаще беспокоить международное сообщество и ООН. В январе 2019 г. департамент по экономическим и социальным вопросом ООН опубликовал доклад, посвященный обзору мирового экономического и социального положения в 2018 г., где сделан вывод о том, что виртуальные активы (криптовалюты) и блокчейн являются важной частью мировой финансовой системы, которые может избавить мир от необходимости доверять централизованным институтам, сократить число бюрократических процедур, создать инновационные бизнес-модели и существенно повысить эффективность управления, изучает возможность использования технологии блокчейн для борьбы с такими явлениями, как преступность, коррупция и особо выделяется борьба с торговлей детьми[140]. Здесь же раскрываются преимущества криптотехнологий, блокчейна и распределенной бухгалтерской книги, а криптовалюта рассматривается как «новый рубеж в области цифровых финансов»[141]. В то же время, по утверждению руководителя Управления ООН по борьбе с распространением наркотиков и преступностью Нила Уолша (30 августа 2019 г.) анонимность криптовалюты мешают борьбе с финансированием терроризма, легализации (отмыванию)

---

[139] *Овчинский В. С.* Основы борьбы с киберпреступностью и кибертерроризмом: хрестоматия / сост. В. С. Овчинский. Москва: Норма, 2017.

[140] Доклад ООН: криптовалюты и блокчейн – это «важная часть глобальной финансовой системы» [Электронный ресурс]. URL: http://cryptoconsulting.info/ru/doklad-oon-kriptovalyutyi-i-blokcheyn-eto-vazhnaya-chast-globalnoy-finansovoy-sistemyi/ (дата обращения: 27.05.2020) (дата обращения: 09.11.2020).

[141] ООН: блокчейн и криптовалюты – новый рубеж в бизнесе и госуправлении [Электронный ресурс]. URL: https://roskomsvoboda.org/44455/ (дата обращения: 09.11.2020); Обзор мирового экономического и социального положения, 2018 год: передовые технологии в интересах устойчивого развития [Электронный ресурс]. URL: https://www.un.org/development/desa/dpad/publication/обзор-мирового-экономического-и-соци/ (дата обращения: 02.05.2020).

преступных доходов и киберпреступностью[142]. Это подтверждается результатами проведенных исследований в рамках ООН, согласно которым сумма легализованных (отмываемых) в мире денежных средств, полученных в результате совершения различного рода преступлений, ежегодно составляет от 2 до 5 % мирового ВВП, или в денежном выражении – от 800 млрд до 2 трлн долларов США[143].

На семьдесят четвертой сессии Генеральной Ассамблеи ООН, которая состоялась 30 июня 2019 г., был принят проект резолюции «Противодействие использованию информационно-коммуникационных технологий в преступных целях», инициатором которой выступила Россия. В ней отражены проблемы как на национальном, так и на международном уровне, а также применяемые меры, направленные на снижение угроз в названной сфере и подчеркнута важность международного сотрудничества в рамках противодействия использованию информационно-коммуникационных технологий в преступных целях[144].

Четырнадцатый Конгресс ООН по предупреждению преступности и уголовному правосудию, который должен был состояться 20–27 апреля 2020 года в Японии (г. Киото), перенесен на сентябрь 2021 г., но в подготовленных и опубликованных материалах проблемам цифровой преступности уделено особое внимание. Так, в соответствии с пунктом 3 статьи 27 Конвенции «об организованной преступности» указано, что государства должны стремиться к укреплению сотрудничества с целью противодействия транснациональной организованной преступности, которая активно при осуществлении преступной деятельности использует современные технологий». Что же касается национального уровня все больше внимания уделяется правовым мерам и укреплению потенциала наряду со стратегическим планированием, что может также включать, в соответствующих случаях, партнерские отношения между государственным и частным сектором. Стремительное развитие инновационных технологий и беспрецедентный прогресс распространения цифровых технологий, таких как искусственный интеллект и робототехника, информатика, технологии распределительного реестра и пр., могут

[142] *Теткин М.* Нил Уолш, ООН [Электронный ресурс]. URL: криптовалюты помогают террористам https://www.rbc.ru/crypto/news/5d68caa79a79472991ab5e9c (дата обращения: 15.09.2020).

[143] Money-Laundering and Globalization [Электронный ресурс] // ООН. URL: http://www.unodc.ogr/unodc/en/money-laundering/globalization.html (дата обращения: 15.03.2020).

[144] Резолюция семьдесят четвертая сессия Генеральной Ассамблеи ООН [Электронный ресурс]. URL: https://www.unodc.org/documents/Cybercrime/SG_report/V1908184_R.pdf.

быть использованы для совершения преступлений. В связи с этим для ООН интересными являются шесть направлений, по которому сегодня международное сотрудничество должно укрепляться и которые между собой тесно взаимосвязаны. К таковым отнесены: использование криптовалюты в преступных целях, незаконный оборот наркотиков, огнестрельного оружия с использованием цифровых технологий, а также связь современных информационных технологий с торговлей людьми, надругательствами над детьми и их эксплуатацией и роль технологий в расследовании дел, связанных с незаконным ввозом мигрантов[145].

Особое внимание ООН уделяет подготовке специалистов правоохранительных органов с целью решения проблем и повышения потенциала для успешного и эффективного расследования и судебного преследования по таким уголовным делам. В связи с этим им отведена большая роль организации конференций и практических семинаров. Проведение таких международных семинаров способствует диалогу и обмену мнениями технического характера относительно вышеуказанных шести тематических областей, представляющих интерес. В ходе их проведения исследуются различные методы, которые используются при совершении преступлений с применением цифровых технологий, и типы таких преступлений; изучаются способы, с помощью которых система уголовного правосудия и правоохранительные органы могут более эффективно предупреждать и выявлять такие преступления, а также бороться с ними как на национальном, так и на международном уровне. При этом изучить успешную практику и проблемы, в связи с современными требованиями, в отношении использования специальных методов расследования и сбора электронных доказательств в случае преступлений, совершаемых с применением цифровых технологий, а также в связи с приемлемостью таких доказательств в суде; провести обзор действующих национальных нормативных стандартов и способствовать дальнейшему обсуждению возможного изменения законодательства, если таковое уместно, для удовлетворения новых потребностей и решения новых проблем и пр.

В пункте 167 материалов семинара-практикума 4. Четырнадцатого Конгресса ООН по предупреждению преступности и уголовному правосудию указывается на важность рассмотрения государ-

[145] Четырнадцатый Конгресс Организации Объединенных Наций по предупреждению преступности и уголовному правосудию Киото, Япония, 20–27 апреля 2020 года [Электронный ресурс]. URL: https://undocs.org/ru/A/RES/69/313 (дата обращения: 20.06.2020).

ствами возможности «разработки междисциплинарных стратегий (включая меры регулирования, директивные инициативы по предупреждению и подготовку сотрудников компетентных органов) с целью решения проблем и повышения потенциала для успешного и эффективного расследования и судебного преследования в соответствующих делах»[146]. По мнению ООН, предложенные меры могут, насколько это возможно в виртуальной среде, способствовать сокращению масштабов незаконных финансовых потоков, связанных с различными формами преступности, включая транснациональную организованную преступность.

Российская Федерация как член ООН является участницей практически всех международных конвенций и соглашений по борьбе с преступностью.

Таким образом, можно констатировать, что на международном уровне ООН предпринят ряд шагов, направленных на разработку правовых основ международного сотрудничества по противодействию цифровой преступности.

10.2. Региональные формы международного сотрудничества в сфере предупреждения цифровой преступности

Региональное сотрудничество в облати противодействия цифровой преступности тоже активизировалось. Так, Советом Европы были приняты Конвенция о преступности в сфере компьютерной информации[147], соответствующая Резолюция[148] и Декларация, направленные на построение безопасного информационного общества[149]. Они сегодня определяют уголовно-правовую политику мирового сообщества, нацеленную на защиту общества от преступлений, совершаемых в сфере цифровых технологий, путем подготовки нор-

[146] Четырнадцатый Конгресс Организации Объединенных Наций по предупреждению преступности и уголовному правосудию Киото, Япония, 20–27 апреля 2020 года [Электронный ресурс]. URL: https://undocs.org/ru/A/RES/69/313 (дата обращения: 20.06.2020).

[147] Конвенция о преступности в сфере компьютерной информации (EST № 185) от 23 ноября 2001 г. (с изм. от 28.01.2003). Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 18.11.2019).

[148] Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности: резолюция A/RES/53/70 от 4 января 1999 г. URL: https://www.ifap.ru/ofdocs/un/5753.pdf (дата обращения: 20.11.2019).

[149] Декларация принципов «Построение информационного общества – глобальная задача в новом тысячелетии» (Женева, 2003) [Электронный ресурс]. URL: https://online.zakon.kz/Document/?doc_id=30170561#pos=7;129 (дата обращения: 20.11.2019).

мативно-правовых актов и укрепления сотрудничества международного сообщества в указанной сфере. В данном документе рекомендовано участникам мирового сообщества предпринимать необходимые организационно-правовые мероприятия, направленные на борьбу с цифровыми преступлениями и предусмотреть в своем законодательстве конкретные составы преступлений в сфере цифровых технологий.

В 2017 году Европарламент принял резолюцию[150] для Еврокомиссии, предложив признать официальный статус машин с искусственным интеллектом, принимающих самостоятельные решения, с возможностью возложения на них ответственности за причиненный ущерб. На практике пока законотворческие инициативы, как в США, так и в Европейском союзе не имеют четкой методологической основы и представляют собой скорее «сборник предложений» по регламентации, без формулирования принципов выбора средств правовой защиты[151].

В январе 2020 года вступила в силу пятая директива ЕС по борьбе с легализацией (отмыванием) преступных доходов (5AMLD)[152], которая ужесточила требования к транзакциям, проводимым с использованием виртуальный актив (криптовалюты) через криптобиржи или цифровые платформы. Криптовалютные платформы теперь обязаны проводить аудит клиента (customer due diligence, CDD) и предоставлять: а) информацию о подозрительных транзакциях (suspicious activity reports, SAR); б) финансовую информацию, адреса владельцев криптокошельков с целью их идентификации; в) криптобиржи должны проходить процедуру государственной регистрации. По мнению авторов директивы, эти меры позволят снизить уровень преступности и анонимности криптодержателей.

Интерпол в своей деятельности придает большое значение информационному обеспечению международного сотрудничества в противодействии отдельным видам преступлений, а именно: легализации (отмыванию) преступных доходов, финансированию терроризма, организованной преступной деятельности, преступлениям, посягающим на экономические и социальные основы жизнедеятельности общества, в том числе в финансовой сфере, и др. Для уста-

---

[150] Резолюция Европарламента от 16 февраля 2017 г. 2015/2013(INL) P8_TA-PROV(2017)0051, включает текст Хартии робототехники [Электронный ресурс]. URL: http://robopravo.ru/riezoliutsiia_ies (дата обращения: 28.11.2019).

[151] *Филипова И. А.* Правовое регулирование искусственного интеллекта: регулирование в России, иностранные исследования и практика // Государство и право. 2018. № 9.

[152] Отмывание денег 2020. 5AMLD: новые правила ЕС по противодействию и BEPS [Электронный ресурс]. URL: https://taxc.com.ua/ (дата обращения: 23.07.2020).

новления местонахождения лиц, участвующих в преступной деятельности Интерполом используется разработанная Генеральным секретариатом специальная система международного обмена информацией. Его роль в координации этой деятельности значительно возросла, поскольку Интерпол, обладая уникальными инструментами и механизмами, методами и практикой противодействия терроризму во всех его формах и проявлениях, цифровой преступности и др., способствует организации содействия государствам-членам, международным организациям, проводит значительную работу по распространению опыта противодействия с этим явлением. Им применяются новые методы и способы работы, поскольку преступники используют в настоящее время самые новые цифровые технологии, стойкую криптографию, позволяющую им уйти от уголовной ответственности. Осложняется работа еще и тем, что зачастую они используют теневой бизнес, в том числе пользуются такими цифровыми площадками, как DarkNet. В связи с этим Интерпол объявил об ужесточении деятельности по противодействию преступности с противоправным использованием криптовалюты в DarkNet, поскольку она является площадкой для хакеров всех типов, мошенников и лиц, осуществляющих незаконный оборот оружия, наркотиков и т. п.[153] В ходе работы по пресечению преступной деятельности в названной сфере ими было заключено партнерское соглашение с южнокорейским стартапом S2W Lab, что позволило, с использованием разработанной ими системы мониторинга активности пользователей DarkNet, которая дает возможность анализировать данные и может выявлять источники подозрительных транзакций, в том числе с криптовалютами, расширить информацию о преступной деятельности.

Большое значение Интерпол уделяет подготовке сотрудников к работе в новых цифровых условиях. С этой целью организуются тренинги по обучению сотрудников Интерпола, непосредственно участвующих в розыске преступности и отслеживающих незаконное использование виртуальных активов «криптовалюты»[154].

Выступая на международном конгрессе, глава Интерпола Мэн Хунвэй заявил, что Интерполом разработана стратегия борьбы с киберпреступлениями, однако имеющиеся методы борьбы с названным видом преступления пока не дают должного эффекта,

---

[153] Обзор: Интерпол усилит борьбу с криминальным использованием криптовалюты в дарквебе [Электронный ресурс]. URL: https://novator.io/blokchejn/interpol-usilit-borbu-s-kriminalnym-ispolzovaniem-kriptovalyuty-v-darkvebe (дата обращения: 16.09.2020).

[154] URL: https://xakep.ru/2015/09/04/interpol-crypto/ (дата обращения: 13.03.2021).

поскольку виртуальный мир преступлений, имея трансграничный и стремительно нарастающий характер, не позволяет своевременно отреагировать на возникающие киберугрозы. Это позволяет добытые преступным путем средства легализовать в течение нескольких часов[155].

По его мнению, в противодействие преступности в сфере цифровой экономики важным является, во-первых, создание электронной платформы для противодействия киберпреступлениям, в котором должны принять участие самые вероятные жертвы хакерских атак – национальные банки и, во-вторых, сотрудничество и взаимодействие со специалистами IT-технологий, провайдерами соответствующих услуг и все те компании, которые связаны с цифровой экономикой. Это позволит полицейским ведомствам каждой страны укрепить связи со своими коллегами[156].

В настоящее время особым приоритетом работы Интерпола является противодействие киберпреступности, связанной с атаками на информационные системы, особенно те, которые следуют бизнес-модели «преступление как услуга» и работают в качестве стимуляторов для онлайн-преступность, борьба с сексуальным насилием над детьми и сексуальной эксплуатацией детей, включая производство и распространение материалов о жестоком обращении с детьми, противодействие мошенничеству и подделке безналичных платежных средств, в том числе крупномасштабное мошенничество с платежными картами (особенно мошенничество с поддельными банковскими картами), преступления, совершаемые с использованием виртуальных активов (криптовалюты).

Уже в 2020 году Интерпол подготовил и опубликовал доклад о преступности в сфере интеллектуальной собственности, который раскрывает особенности деятельности организованной преступности в этой сфере. Это обусловлено тем, что распространение контрафактных товаров нарушает права граждан, а посягательства на интеллектуальную собственность причиняют вред экономике в целом и компаниям, владельцам интеллектуальной собственности, а также могут нанести ущерб здоровью и благополучию потребителей.

Тематические исследования, представленные в настоящем докладе, иллюстрируют, как широкий спектр различных преступлений связан с преступлениями в области интеллектуальной соб-

---

[155] *Давыдов Д.* Интерпол придумал, как бороться с киберпреступностью [Электронный ресурс]. URL: https://teknoblog.ru/2018/07/06/90797 (дата обращения: 05.04.2021).

[156] *Там же.*

ственности, включая незаконный оборот оружия и наркотиков, экономические и финансовые преступления, а также различные виды мошенничества, легализацию (отмывание) преступных доходов, фармацевтические преступления, производство и распространение контрафактной продукции, принудительный труд, коррупцию с использованием виртуальных активов (криптовалюты).

Заметна активная работа, проводимая Европолом в сфере противодействия цифровой преступности[157]. Начиная с 2014 года ежегодно он представляет доклад «Оценка угрозы со стороны организованной интернет-преступности», который пополняется новой информацией о киберпреступности, а также рассматриваются инструменты для обеспечения преступности «глубокого» интернета, в том числе и сексуальной эксплуатации детей, анонимность услуг которых обеспечивается такими цифровыми платформами как Tor. Это свидетельствует о том, что правоохранительные органы не всегда могут отследить крупные сделки, совершаемые с использованием криптовалют, поскольку транзакции обеспечены высокой анонимностью, что способствует росту таких преступлений. В большинстве случаев противоправное использование виртуальных активов (криптовалют) связывают преимущественно с легализацией (отмыванием) преступных доходов, что послужило основанием создания в 2016 г. по инициативе Европейской комиссии на базе Европола специальной рабочей группы, которая непосредственно занимается борьбой с легализацией (отмыванием) преступных доходов с использованием виртуальных активов (криптовалют)[158].

Одним из проектов Европола является консультативная группа SOCTA (Serious and Organized Crime Threat Assessment), в состав которой входят государства-члены ЕС, агентства ЕС, Европейская комиссия и Генеральный секретариат Совета. Особое внимание SOCTA уделяется противодействию организованной преступной деятельности. Представители организованной преступности «внедряют и интегрируют новые технологии в свой modus operandi или создают совершенно новые бизнес-модели вокруг них. Использование новых технологий ОПГ оказывает влияние на преступную деятельность по всему спектру серьезной и организованной преступности. В первую очередь, это относится

[157] *Быкова Е. В.* Проблемы и перспективы сотрудничества Российской Федерации с международными организациями в сфере уголовного судопроизводства // Международное уголовное право и международная юстиция. 2016. № 5.

[158] *Асмаков А.* Европол и Интерпол объединили усилия в борьбе с отмыванием денег через криптовалюты [Электронный ресурс]. URL: https://forklog.com/evropol-i-interpol-obedinili-usiliya-v-borbe-s-otmyvaniem-deneg-cherez-kriptovalyuty/ (дата обращения: 09.03.2021).

к цифровому криминалу, широко использующему масштабирование онлайн-торговли и повсеместное распространение зашифрованных каналов связи»[159]. Ими активно применяется криптовалюта, поскольку скоростная обработка транзакций и распространение эффективных средств анонимности оказывают большую помощь организованной преступности в легализации (отмывании) преступных доходов.

Европолом в деятельности по противодействию транснациональной организованной преступности активно применяется система раннего обнаружения организованных преступных групп (ОПГ) с использованием методов вычислительного сканирования и разведывательных систем – ePOOLICE. Благодаря ей создается эффективная общеевропейская система «средового сканирования для предупреждения готовящихся к преступлениям действующих и возникающих ОПГ»[160]. Уже создана «система сплошного мониторинга, включающая сбор информации из интернета, социальных сетей, из каналов части мессенджеров, информации о финансовых транзакциях, биллинговая информации, видеопотоков и т. п.»[161]. Информация также включает такие данные как текстовой и видео- контент, финансовые данные и пр., что позволяет анализировать полученные данные всесторонне и своевременно реагировать на вызовы транснационального криминала.

Европол осуществляет большую представительскую работу, проводя международные конференции, а также совместно с Интерполом проводят и совместные семинары, позволяющие объединить усилия по противодействию преступной деятельности с использованием цифровых технологий.

Рост организованной преступности в сфере экономики и финансов, а также число обращений со стороны государств-членов ЕС с просьбой об оперативной поддержке, способствовали созданию в штаб-квартире Европола Европейского центра по борьбе с финансовыми и экономическими преступлениями (EFECC)[162].

---

[159] *Ларина Е.С.* Искусственный интеллект. Большие данные. Преступность / Е. С. Ларина, В. С. Овчинский / («Коллекция Изборского клуба»). Москва: Книжный мир, 2018. С. 207.

[160] *Там же.*

[161] *Там же.*

[162] Он создан по образцу аналогичных инициатив, таких как Европейский центр по борьбе с киберпреступностью (EC3), Европейский Контртеррористический центр (ECTC), Европейский центр по незаконному ввозу мигрантов (EMSC) и Европейский центр по борьбе с серьезными организованными преступлениями (ESOCC), размещенный в Европоле (см. URL: https://www.europol.europa.eu/newsroom/news/europol-launches-european-financial-and-economic-crime-centre) (дата обращения: 22.12.2021).

В рамках этой программы расследование, проведенное в 2016 году при поддержке Европола, Евроюста (Eurojust) и других организаций, показало, что более 90 % операций, проведенных денежными мулами, связаны с киберпреступностью. Незаконно полученные деньги часто поступают от фишинга, вредоносных атак, мошенничества с платежными картами и с онлайн-покупками/электронной коммерцией и др.

Так, в течение недели Европейский центр по борьбе с киберпреступностью Европола (EC3) и совместная целевая группа по борьбе с киберпреступностью (J-CAT) совместно с Евроюстом (Eurojust) и европейской банковской Федерацией (EBF) оказывали оперативную и аналитическую поддержку соответствующим органам власти. Эта операция привела к идентификации почти 700 денежных мулов по всей Европе. Полиция допросила 198 подозреваемых и произвела 81 арест. Эта операция была частью европейского проекта Money Mule Action (EMMA), пилотного проекта, проводимого в рамках оперативного плана действий EMPACT по борьбе с киберпреступностью и мошенничеством с платежными картами, направленного на борьбу с мошенничеством в интернете и платежными картами. Она позволила сделать вывод, согласно которому помимо организованных преступных групп, легализацией (отмыванием) преступных доходов занимаются профессионалы, оказывающие эти услуги от имени других лиц. Масштабы легализации (отмывания) преступных доходов трудно оценить, но они считаются значительными. По оценкам Управления ООН по наркотикам и преступности (УНП ООН), ежегодно отмывается от 2 до 5 % мирового ВВП. Это от 715 млрд до 1,87 трлн евро ежегодно[163].

3 июля 2018 г. ознаменовалось тем, что было объявлено о создании альянса пяти стран – Joint Chiefs of Global Tax Enforcement (J5) – Международный альянс J5 по борьбе с серьезными международными преступлениями. Его особенность в том, что это оперативное сотрудничество между пятью странами (Австралия, Канада, Нидерланды, Великобритания и США) заключается в организации деятельности, направленной на борьбу с транснациональными финансовыми преступлениями, в том числе с использованием виртуальных валют (криптовалют). В рамках альянса J5 предполагается «партнерство между Австралийской комиссией по уголовным расследованиям (ACIC) и Налоговой службой Австралии (ATO),

[163] URL: https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/economic-crime/money-laundering (дата обращения: 11.04.2021).

Канадским налоговым агентством (CRA), Fiscale Inlichtingen-Opsporingsdienst (FIOD) в Нидерландах, Королевской налоговой и таможенной службы Великобритании (HMRC) и Налоговой службой США (IRS)»[164]. Целью его создания стало укрепление правопорядка, путем обмена информацией и ресурсами; развитие международного сотрудничества по борьбе с легализацией (отмыванием) преступных доходов и финансовыми преступлениями, а также преступлениями, совершаемыми с использованием виртуальных активов (криптовалют); повышение эффективности работы организации по экономическому сотрудничеству и развитию с применением новых подходов и проведение совместных расследований; совместная разработка и выработка новых подходов к расследованию преступлений и подготовке совместных операций; обнаружение и устранение международных преступных схем и инструментов, способствующих совершению преступлений, совершаемых с использованием виртуальных активов (криптовалют); повышение уровня обмена информацией, пилотными программами; совместные криминальные расследования[165].

Наряду с другими организациями деятельность на международном уровне проводит и Группа разработки финансовых мер по борьбе с отмыванием денег (Financial Action Task Force, FATF). Ею в последние годы активизировалась работа по противодействию легализации (отмывания) преступных доходов и финансированию терроризма, так как не только возросло количество этих преступлений во всем мире, но и появились новые инструменты, с использованием которых осуществляется легализация. В связи с этим только за 2013–2014 гг. ею подготовлены руководства по 152 применениям риск-ориентированного подхода в отношении предоплаченных карт, мобильных платежей и систем платежей через Интернет, в том числе и с использованием криптовалют[166].

---

[164] Пять стран начинают совместную борьбу с финансовыми преступлениями с участием криптовалют [Электронный ресурс]. URL: https://bits.media/pyat-stran-nachinayut-sovmestnuyu-borbu-s-finansovymi-prestupleniyami-s-uchastiem-kriptovalyut/ (дата обращения: 08.11.2020).

[165] Международный альянс J5 будет бороться с «криптовалютной угрозой» в сфере отмывания денег и уклонения от налогов [Электронный ресурс]. URL: https://news.myseldon.com/ru/news/index/191224059; США возглавили международный альянс силовиков по борьбе с отмыванием денег [Электронный ресурс]. URL: https://hashtelegraph.com/ssha-vozglavili-mezhdunarodnyj-aljans-cilovikov-po-borbe-s-otmyvaniem-deneg/ (дата обращения: 20.12.2020).

[166] Руководство по применению риск-ориентированного подхода. Предоплаченные карты, мобильные платежи и онлайн платежи [Электронный ресурс] / пер. МУМФЦМ // ФАТФ. 2013. URL: http://www.eurasiangroup.org/files/FATF_

За последние годы ФАТФ обращала неоднократно внимание на проблемы идентификации личности Так, например, ею подготовлено Руководство «О цифровой идентификации личности», которое в марте 2020 г. было направлено во все страны участницы[167]. Основанием этому является тот факт, что цифровые платежи растут ежегодно (в среднем на 12,7 %) и, по прогнозам, количество транзакций за год может достичь 726 миллиардов, а к 2022 году, по оценкам экспертов, 60 % мирового ВВП будет оцифровано. С ростом числа цифровых финансовых операций, по мнению ФАТФ, требуется более глубокое понимание того, как отдельные лица могут выявляться и проверяться в мире цифровых финансовых услуг.

Благодаря деятельности ФАТФ была принята Декларация «Большой двадцатки» (G20) «Создание консенсуса для честного и устойчивого развития», которая стала результатом работы 13-й встречи представителей государств, входящих в «Большую двадцатку», прошедшей с 30 ноября по 1 декабря 2018 г. в Буэнос-Айресе (Аргентина). Она включала к рассмотрению такие вопросы как регулирование рынков виртуальных активов (криптовалют) в контексте «открытой и устойчивой финансовой системы», которая «важна для поддержания устойчивого роста»[168].

ФАТФ в июне 2018 г. приступила к корректировке руководящих указаний и Стандартов, которые ею ранее были подготовлены с целью определения необходимости их изменения не только в связи с ростом использования криптовалют и иных виртуальных активов, но и определения рисков, которые они несут. В середине 2019 г. ею вносятся поправки в Рекомендацию 15, согласно которым устанавливаются дополнительные требования, касающиеся базовых обязательств по применению риск-ориентированного подхода в отношении новых технологий. ФАТФ предлагает помимо выявления и проведения оценки рисков легализации (отмывания) преступных доходов и финансирования терроризма, связанных с разработкой

---

docs/Rukovodstvo_FATF_po_primeneniyu_riskorientirovannogo_podhoda_dlya_predoplachennyh_kart_mobilnyh_platezhej_i_onlajn_platezhej_2013. pdf (дата обращения: 24.07.2020); Виртуальные валюты: ключевые определения и потенциальные риски в сфере ПОД/ФТ [Электронный ресурс] / пер. МУМФЦМ // ФАТФ. 2014. URL: http://www.eurasiangroup.org/files/FATF_docs/Virtualnye_valyuty_FATF_2014. pdf (дата обращения: 18.07.2020).

[167] О цифровой идентификации личности: руководство от 6 марта 2020 г. [Электронный ресурс]. URL: www.fatf-gafi.org/ (дата обращения: 02.06.2020).

[168] Итоги Саммита G20: криптовалюты важны для глобальной экономики, но необходимо регулирование и налогообложение [Электронный ресурс]. URL: https://btcinfor.com/mine/itogi-sammita-g20-kriptovaluty-vajny-dlia-globalnoi-ekonomiki-no-neobhodimo-regylirovanie-i-nalogooblojenie.html (дата обращения: 03.03.2021).

новых продуктов и новой деловой практики, включать новые механизмы распространения и использования новых или развивающихся технологий. В этой связи необходимо, чтобы финансовые учреждения стран-участниц, получившие лицензию или осуществляющие деятельность в их юрисдикции, «приняли соответствующие меры для управления и снижения рисков до запуска новых продуктов, внедрения новой деловой практики или использования новых или развивающихся технологий. При этом требования, касающиеся новых технологий, должны распространяться на платежные продукты и услуги на основе виртуальной валюты»[169].

Здесь же указывается на необходимость повышения эффективного регулирования, контроля и мониторинга деятельности провайдеров (поставщиков) услуг в сфере оборота виртуальных активов и финансовой деятельности с использованием виртуальных активов[170].

Предпринятые меры и предложения организации, основанные на анализе совершаемых преступлений явились обоснованием создания комплекса специальных рекомендаций для правоохранительных органов по расследованию преступлений, при совершении которых виртуальные валюты выступают средством совершения преступлений, в том числе перемещения преступных активов в иностранные юрисдикции, легализации (отмывания) преступных доходов и финансирования терроризма. Более того, здесь же высказаны требования к странам, которые должны соблюдать соответствующие рекомендации ФАТФ по предотвращению неправомерного использования виртуальных активов.

На этом фоне ФАТФ создало контактную группу контроля за качеством соблюдения стандартов ФАТФ и более эффективной защиты международной финансовой системы от злоупотреблений. Эти изменения в деятельности ФАТФ были поддержаны и одобрены на встрече G20 в Фукуоке. В свою очередь ФАТФ продолжила свою деятельность по обеспечению эффективного регулирования и надзора за использованием новых технологий, в том числе в контексте виртуальных активов, в целях снижения связанных с этим рисков легализации (отмывания) преступных доходов и финансирования терроризма и поддержки ответственных инноваций в секторе финансовых услуг.

---

[169] Виртуальные валюты. Руководство по применению риск-ориентированного подхода. Июль 2015 г. [Электронный ресурс]. URL: http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf (дата обращения: 28.03.2020).

[170] Публичное заявление о виртуальных активах и связанных с ними провайдерах (дата обращения: 12.06.2020) [Электронный ресурс]. URL: http://www.fedsfm.ru/content/files/bulleten38_ru_print.pdf / (дата обращения: 15.03.2021).

Кроме того, в рамках этой проблемы в ноябре 2019 г. опубликован проект рекомендаций по развертыванию систем цифровой идентификации[171], которые направлены на анализ особенностей работы криптовалютных и блокчейн-компаний, с целью обеспечения соблюдения правил борьбы с легализацией (отмыванием) преступных доходов и противодействия финансированию терроризма.

Между тем, ФАТФ предлагает государствам-участникам на национальном уроне принять «руководящие принципы или нормативные акты, позволяющие надлежащим образом использовать независимые системы цифровой идентификации организациями, регулируемым для целей AML/CFT». Помимо названных принципов и нормативных документов регулируемым учреждениям, например, криптовалютным биржам, предлагается «использовать информированный подход с учетом оценки рисков в случае развертывания систем цифровой идентификации для надлежащей проверки клиентов»[172].

К концу первой половины 2020 г. этот проект был дополнен рядом рекомендаций и уже опубликован в новой редакции. Так, были включены, например, положения обязывающее операторов криптовалютных сервисов (в первую очередь, криптовалютных бирж), передавать информацию о клиентах при совершении ими переводов не только в фиатных валютах, но и о криптовалютных транзакциях. Такое решение ФАТФ при принятии этих рекомендаций «регуляторами стран, в которых зарегистрированы крупнейшие биржи криптовалют, сильно встряхнет рынок и осложнит работу как биржам, так и трейдерам»[173].

На пленарной сессии ФАТФ, которая состоялась 8–24 июня 2020 г. было уделено внимание снижению рисков легализации (отмывания) преступных доходов и финансирования терроризма с использованием виртуальных активов, в том числе и «стейблкоинами», который может рассматриваться как виртуальный или как традиционный финансовый актив. Ключевое отличие стейблкоинов

---

[171] FATF опубликовала рекомендации по развертыванию систем цифровой идентификации [Электронный ресурс]. URL: https://bits.media/fatf-opublikovala-rekomendatsii-po-razvertyvaniyu-sistem-tsifrovoy-identifikatsii/ (дата обращения: 27.05.2020).

[172] Применение риск-ориентированного подхода для банковского сектора: руководство ФАТФ [Электронный ресурс]. URL: file://E:/междугородка%20крипта/rukovodstvo_fatf_rop_v_bankovskom_sektore.pdf (дата обращения: 28.05.2020 г.).

[173] Сегодня группа FATF опубликовала финальную версию рекомендаций по регулированию криптовалют и деятельности операторов криптовалютных сервисов [Электронный ресурс]. URL: https://bits.media/finalnaya-versiya-rekomendatsiy-fatf-birzhi-kriptovalyut-budut-obyazany-obmenivatsya-informatsiey-o-/ (дата обращения: 07.07.2020).

от «стандартных» виртуальных активов заключается в том, что они обладают «потенциалом повсеместного распространения ввиду их бóльшей привлекательности (более высокая стабильность, безопасность операций и простота использования по сравнению со «стандартными» виртуальными активами), что одновременно повышает вероятность их использования преступными элементами»[174].

Все вышеизложенное свидетельствует о значительном объем работы, которая проделана Группой разработки финансовых мер борьбы с отмыванием денег (ФАТФ) с момента ее создания в сфере противодействия легализации (отмывании) преступных доходов, финансирования терроризма и предотвращения финансирования распространения оружия массового уничтожения.

Имеющаяся правовая база в сфере киберпространства и противодействия киберпреступности[175] в полной мере не отвечает современным требованиям и требует консолидации мирового сообщества к принятию единых правил игры как в повседневном использовании криптовалюты, так и в противодействии преступлениям, с ее криминальным оборотом.

Краткий анализ деятельности в сфере предупреждения цифровой преступности международных органов и организаций, позволил прийти к выводу о том, что в этом направлении практика противодействия цифровой преступности только складывается, существуют проблемы правового характера, поскольку нет еще сложившегося понимания сущности цифровых технологий, а особенно виртуальных валют (криптовалют), отсутствуют методические рекомендации по расследованию этих преступлений, нет законодательного определения на региональном уровне.

---

[174] Обзор событий в сфере противодействия отмыванию доходов, полученных преступным путем и финансированию терроризма. 1–30 июня 2020: Банк России. Июнь 2020.

[175] Кибербезопасность и управление Интернетом: документы и материалы для российских регуляторов и экспертов / отв. ред. М. Б. Касенова; сост. О. В. Демидов и М. Б. Касенова. Москва: Статут, 2013; Electronic Communications Privacy Act of 1986 [Электронный ресурс] // ECPA. URL: http://dorothy.as.arizona.edu/ LAW/ref5.html (reference date: 05/05/2019); The National Strategy to Secure Cyberspace [Электронный ресурс]. URL: http://www.whitehouse.gov/pcipb/ (reference date 15/04/2019; State Cybersecurity Strategies. URL: https:// www.securitylab.ru (reference date: 05/05/2019); Site of the Council of Europe. URL: https: // search.coe.int (reference date: 25/05/2019); *Волеводз А. Г.* Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. Москва: Юрлитинформ, 2001; *Желудков М. А.* Особенности реализации в России международного опыта по защите от корыстных преступлений, совершаемых в киберпространстве // Вестник экономической безопасности. 2016. № 5; Информационный ресурс «China Space» [Электронный ресурс]. URL: http://www.chinaspace.ru (дата обращения: 06.05.2019).

Контрольные вопросы

1. Определите роль ООН в создании правовых основ предупреждения цифровой преступности.
2. Что является основой международного сотрудничества в сфере предупреждения цифровой преступности?
3. Назовите основные направления Интерпола в деятельности по предупреждению цифровой преступности.
4. Определите роль Европола в деятельности по предупреждению цифровой преступности.

ОСОБЕННАЯ ЧАСТЬ

Глава 11. Криминологическая характеристика преступной деятельности с использованием виртуальных активов (криптовалюты)

Планируемые результаты освоения темы главы

– **знать** особенности преступности в сфере оборота виртуальных активов (криптовалют), как социального явления; понимать характерные ее особенности;

– **уметь** применять свои знания для понимания закономерностей и тенденций развития преступности в сфере оборота виртуальных активов (криптовалют); при анализе современного состояния этого вида преступности, использовать статистические показатели и выстраивать цепочку к изучению приичн и условий, способствующих их совершению; ориентироваться в особенностях определения латентной преступности и социальных последствий;

– **владеть** терминологией преступности в сфере оборота виртуальных активов (криптовалют); навыками для организации и проведения криминологических исследований; прогнозирования этого вида преступности, планирования профилактических мероприятий.

11.1. Международный и зарубежный опыт противодействия преступной деятельности в сфере оборота виртуальных активов (криптовалют)

В современном информационном обществе применение цифровых технологий способствовало развитию виртуальных экономических отношений, в том числе электронной коммерции, которая способствовала развитию электронных платежных сервисов с целью использования электронных денег, а активное развитие цифровых технологий создание распределительного реестра способствовало развитию и распространению во всем мире виртуальных активов (криптовалют).

Исследование международного и зарубежного опыта противодействия преступной деятельности с использованием виртуальных активов (криптовалюты) позволит идентифицировать ключевые

проблемы, связанные с противодействием преступности как за рубежом, так и в России.

В настоящее время большое внимание виртуальным активам (криптовалюте) уделяет и Организация объединенных наций (ООН). Так, в январе 2019 г. на своем официальном сайте размещен доклад, посвященный обзору мирового экономического и социального положения в 2018 г., где сделала вывод, что виртуальные активы (криптовалюты) и блокчейн являются важной частью мировой финансовой системы, которые могут избавить мир от необходимости доверять централизованным институтам, сократить число бюрократических процедур, создать инновационные бизнес-модели и существенно повысить эффективность управления. В то же время ООН изучает возможность использования технологии блокчейн для борьбы с такими явлениями, как преступность, коррупция и особо выделяется борьба с торговлей детьми. Помимо этого, виртуальные активы (криптовалюты) рассматривают как «новый рубеж в области цифровых финансов».

Организация объединенных наций открывает фонд для финансирования цифровыми токенами, а его французское подразделение ЮНИСЕФ начинает принимать пожертвования в девяти виртуальных активах (криптовалютах). В соответствии с международной программой «Цели устойчивого развития», признанной решить такие глобальные проблемы, как бедность, неравенство, климатические изменения, ухудшение состояния окружающей среды и т. д. Специально под эту программу создан фонд, который должен привлечь несколько сотен миллионов долларов и разместить их как в фиатном, так и в цифровом формате в системе блокчейн. Фонд станет первой структурой в составе программы ООН, которая сможет принимать и работать со всеми видами криптовалютных и цифровых активов. Известно, что управлять фондом будет децентрализованная платформа кредитования Celsius Network, а запускать проект будет поставщик финансовых услуг Fifth Element. В рамках этой программы французское подразделение Международного детского фонда ООН (ЮНИСЕФ) объявило о том, что начнет принимать пожертвования в девяти криптовалютах: Bitcoin, Bitcoin Cash, Ethereum, Litecoin, XRP, EOS, Monero, Dash и Stellar. Более того, ЮНИСЕФ уже применяет вычислительные мощности компьютеров для сбора пожертвований с помощью майнинга виртуальной валюты (криптовалюты) Monero.

К сожалению, в настоящее время нет базовых документов на международном уровне, положенных в основу формирования нормативно-правовых актов и направленных на противодействие

преступной деятельности с использованием виртуальной валюты (криптовалюты).

Международный валютный фонд (МВФ) несмотря на то, что рассматривает применение в современной экономике виртуальные валюты (криптовалюты) как финансовый актив, подчеркнул, что они могут использоваться для легализации (отмывания) преступных доходов, финансирования терроризма, уклонения от уплаты налогов и мошенничества. Именно по этой причине, по мнению названного фонда, нельзя легкомысленно относиться к правовому регулированию виртуальных активов (криптовалюты), так как масштабные изменения в финансовых системах будут ощутимы.

При этом следует признать, что изучение развития зарубежного законодательства в сфере противодействия преступной деятельности с использованием виртуальных активов (криптовалюты) и рассмотрение проблем ее правового регулирования для деятельности правоохранительных органов стран мира и России имеет особое значение, поскольку масштабы ее распространения и рост преступлений с ее использованием очевиден. Так, например, по данным Group-IB, CipherTrace, CarbonBlack, в 2018 году хакеры совершили хищения виртуальных активов (криптовалют) на сумму от $1.1 до $1.7 миллиарда, из которых $960 миллионов — у криптобирж и платежных систем. Количество таких случаев выросло в 3.5 раза по сравнению с 2017 годом, и в 7 раз по сравнению с 2016 годом. 56 % крипто-краж пришлись на биржи Южной Кореи и Японии. Самые крупные хищения приходится на 2018 год: $532 миллиона у Coincheck; $60 миллионов у Zaif; $40 миллионов у Coinrail; $31 миллион у Bithumb[176].

Особое внимание распространению преступлений, совершаемых с использованием виртуальных активов (криптовалюты) в своей деятельности уделяется такими ведомствами как Интерпол и Европол. По мнению представителей Европола, имеет место быть угроза массового незаконного ее использования в преступных целях, что требует особого подхода, особых знаний в расследовании таких преступлений, уделяя особое внимание выявлению использования виртуальных активов (криптовалют) организованными преступными сообществами. При этом в своей деятельности он собирает информацию, оказывает помощь и в рассле-

[176] *Sikirin V.* Cryptocurrencies and crime: what statistics say [Электронный ресурс]. URL: https://decenter.org/ru/kriptovalyuty-i-prestupnost-chto-govorit-statistika (accessed: 28.01.2020).

довании такой преступной деятельности, как торговля людьми, где она, в последнее время, стала особенно популярной среди торговцев людьми, так как преступникам помогает анонимность, которая обеспечивается виртуальные активы (криптовалютой), а также скорость, с которой осуществляются транзакции, что значительно замедляет процесс отслеживания транзакций и поиска подозреваемых.

К таким преступлениям можно отнести и незаконный оборот наркотиков. Примером может служить деятельность Европола 2018 г. по раскрытию схемы незаконного оборота наркотиков, в которой для отмывания денежных средств в сумме более 8 млн евро через финскую биржу использовались криптовалюты и кредитные карты. Это позволило им арестовать 11 человек за отмывание денежных средств из Испании в Колумбию при помощи виртуальных активов (криптовалюты) и кредитных карт, а правоохранительным органам Испании, Финляндии и США общими усилиями осуществить арест подозреваемых. Благодаря этим мероприятиям была расследована преступная деятельность 137 человек, в ходе которой использовалось 174 банковских счета.

В связи с этим представители ведомства заявили, что Европол «будет продолжать координировать действия между государствами-членами ЕС и за его пределами в стремлении эффективно реагировать на эту растущую угрозу».

Декларация «Большой двадцатки» (G20) «Создание консенсуса для честного и устойчивого развития», которая стала результатом работы 13-й встречи представителей государств, входящих в «Большую двадцатку», прошедшей с 30 ноября по 1 декабря 2018 г. в Буэнос-Айресе (Аргентина), включает вопросы регулирования рынков виртуальных активов (криптовалют) в контексте «открытой и устойчивой финансовой системы», которая «важна для поддержания устойчивого роста». Вместе с тем, отмечается в документе «Мы будем регулировать криптоактивы для борьбы с отмыванием денег и противостояния финансированию терроризма в соответствии со стандартами FATF, и рассмотрим другие меры при необходимости». Государства-члены G20 заявляли о необходимости международной дискуссии о новой индустрии. При этом члены G20 обратились к FATF о подготовке своих стандартов для криптовалютных рынков в странах-членах и способствовать их внедрению. FATF в свою очередь считает, что виртуальные активы (криптовалюты) способствуют не только бесконтрольному отмыванию преступных доходов и финансированию терроризма, но и применению ее при совершении других преступлений.

На международном уровне, как один из методов противодействия легализации (отмыванию) отмыванию преступных доходов и финансированию терроризма FATF в октябре 2018 года заявил о том, что к июню 2019 года государства будут обязаны лицензировать или регулировать криптовалютные биржи и некоторые компании, такие как провайдеры криптовалютных кошельков.

Более того, FATF выдвинул дополнительные требования, согласно которым странам предлагается при внедрении новых цифровых технологий, обязывать финансовые учреждения, получившие лицензию принимать меры для управления рисками и их снижению еще до внедрения новых технологических продуктов и деловой практики. Особое внимание, по мнению FATF, должно уделяться платежным продуктам и услугам на основе виртуальной валюты[177]. Также ФАТФ издается Методология[178] для проведения оценки соответствия систем противодействия легализации (отмыванию) преступных доходов и финансированию терроризма, которая к 2020 году была обновлена и в ней закреплены критерии технического соответствия и эффективности национальных систем противодействия легализации (отмыванию) преступных доходов и финансирования терроризма[179].

За последние годы ФАТФ неоднократно обращала внимание на проблемы идентификации личности. Ею подготовлено Руководство «О цифровой идентификации личности», которое с 6 марта 2020 г. было направлено во все страны – участницы[180]. Основанием этого явился факт ежегодно роста цифровых платежей (в среднем на 12,7 %) и прогноз количество транзакций, который за 2020 г. может достичь 726 миллиардов, а к 2022 году, по оценкам экспертов, 60 % мирового ВВП будет оцифровано.

Все вышеизложенное свидетельствует о том, что имеющаяся правовая база в сфере киберпространства и противодействия

---

[177] Виртуальные валюты. Руководство по применению риск-ориентированного подхода. Июль 2015 г. [Электронный ресурс]. URL: http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf (дата обращения: 08.09.2019).

[178] Methodology for assessing technical compliance with the FATF Recommendations and the effectiveness of AML/CFT systems [Electronic resource] // FATF. Paris, 2013. URL: http://www.fatf-gafi.org/media/fatf/ documents/methodology/FATF%20 Methodology%2022%20Feb%202013.pdf (accessed: 25.03.2013). 3Ibid.

[179] Methodology for assessing technical compliance with the FATF Recommendations. P. 13. 2Ibid; *Мелкумян К. С.* Эффективность деятельности Группы разработки финансовых мер борьбы с отмыванием денег (ФАТФ) в противодействии финансированию терроризма: дис. ... канд. полит. наук. 2019.

[180] О цифровой идентификации личности: руководство от 6 марта 2020 г. [Электронный ресурс] // ФАФТ, 2020. URL: www.fatf-gafi.org/ (дата обращения: 02.06.2020).

названным видам преступности в полной мере не отвечает современным требованиям и требует консолидации мирового сообщества к принятию единых правил игры как в повседневном использовании виртуальных активов (криптовалют), так и в противодействии преступлениям, с ее криминальным оборотом.

В то же время, для того чтобы противодействовать использованию виртуальных активов (криптовалют) в преступных целях, необходимо определиться с направлениями правового регулирования отношений, связанных с их оборотом.

Вместе с тем в первой половине 2018 г. в целях совместного расследования деятельности международных преступных групп, включая легализацию (отмывание) преступных доходов и финансирование преступной деятельности с использованием виртуальных активов (криптова-лют) представители финансовых разведок и налоговых органов США, Австралии, Канады, Нидерландов и Великобритании создали международный оперативный альянс J5 (Joint Chiefs of Global Tax Enforcement). В его рамках они готовы осуществлять обмен информацией и совместно выработать и протестировать новые подходы к противодействию такого рода преступлениям, совместно разрабатывать современные подходы к расследованию преступлений и подготовке совместных операций.

В январе 2020 г. вступила в силу Пятая директива Евросоюза о противодействии легализации (отмыванию) преступных доходов[181], которая выработала новые правила и ужесточила требования к криптовалютным платформам, согласно которым криптовалютные биржи, провайдеры криптокошельков и поставщиков услуг по хранению данных обязаны зарегистрироваться у местного регулятора, представлять отчеты о подозрительной деятельности и выполнять правовой аудит клиента. Такое решение позволит в будущем повысить доверие к криптовалютному рынку со стороны традиционных финансовых институтов и привлечь институциональных инвесторов к стремительно развивающемуся рынку.

И несмотря на то что правовой статус виртуальных активов (криптовалют) не определен, ее оборот легализован на всей территории Евросоюза, она, как разновидность виртуальной цифровой валюты, приобрела высокую популярность и в ряде таких стран мира, как Великобритания, Япония, Швейцария, Швеция, Герма-

[181] URL: https://eur-lex.europa.eu/le_qaIcontenVEN/TXT/?uri:uriserv:OJ.L]0.07.2020)20l8,l56.0 l -004з.0 l.ENG&toc= OJ:L; 20 l8: l56:TOC (дата обращения: 15.07.2021).

ния и др. «стала не только полноценным платежным средством, но и выступает инвестиционным активом»[182].

Так, считается, что Великобритания в настоящий момент является одной из благоприятных для использования системы распределительного реестра (блокчейна) стран в части отсутствия правовых барьеров и поддержки стартапам, которые связаны с виртуальными активами (криптовалютами).

Рабочей группой при правительстве Великобритании, опубликован масштабный доклад, обозначены приоритетные направления правового регулирования технологий блокчейна и оборота виртуальных активов (криптовалют). Наиболее ключевыми из них являются: утверждение правил ICO в Британии и запретов в целях профилактики использования ее в преступной деятельности. На законодательном уровне правовой статус криптовалюты пока еще не определен. Каких-либо специальных запретов и регламентов оборота виртуальных активов (криптовалют) законодательство Великобритании не содержит. Правовые барьеры оборота специально не направлены на ограничение оборота виртуальных валют (криптовалют), а являются общими применительно к противодействию преступной деятельности, в которой виртуальные активы могут использоваться.

Германия одна из первых европейский стран, которая занялась регулированием криптовалютных отношений на нормативном уровне. Несмотря на то что в 2013 году Министерство финансов Германии, отвечающее за законодательство в области виртуальных активов (криптовалют), издало постановление о признании биткоина официальным средством расчетов, она не может быть квалифицирована как иностранная валюта или безналичные деньги. С учетом изменений в указанный нормативный акт 2017 г. биткоин квалифицируется как «финансовый инструмент» и имеет статус частных денег, что позволяет использовать виртуальный актив лишь в расчетах между частными лицами. В гражданском обороте она может участвовать как средство платежа в операциях между частными лицами, конвертироваться в фиатные валюты и может выступать в качестве товара при совершении гражданско-правовых сделок. Если с момента приобретения виртуальных активов (криптовалюты) до ее реализации не прошло 12 месяцев, то в этом случае начисляется налог с продажи. В остальных случаях, получен-

[182] *Пинкевич Т. В.* Проблемы обеспечения безопасности цифровых технологий в Российской Федерации / Т. В. Пинкевич, А. В. Нестеренко // Вестник Костромского государственного университета. 2019. Т. 25. № 4.

ный доход в результате роста капитализации виртуальных активов (криптовалюты), налогообложению не подлежит.

Уголовное законодательство Германии не содержит специальных норм об ответственности за посягательства в сфере оборота виртуальных активов (криптовалют). В то же время правоохранительная система этой страны уделяет существенное внимание в области охраны прав инвесторов, в том числе в криптовалютной сфере.

В Швеции виртуальные активы (криптовалюты) признаны в качестве валюты и могут быть не только предметом сделок по передаче имущества в собственность, в займы, в залог, но и быть расчетным средством. Ее оборот между частными лицами осуществляется в свободной форме. В отношении виртуальной валюты (криптовалюты) не применяется налог на добавленную стоимость и доход на ее приобретение в личных целях. В то же время применяется налог с дохода на прирост капитала.

Уголовное законодательство не содержит специальных норм, устанавливающих уголовную ответственность за нарушение имущественных отношений, связанных с оборотом виртуальных активов (криптовалют).

Безусловно Соединенные Штаты Америки являются страной, где виртуальные активы (криптовалюты) получили широкое распространение. Деятельность, связанную с виртуальными валютами (криптовалютами) осуществляет ряд ведомств, которые ее регулируют[183], в то же время единообразного определения статуса виртуальных активов (криптовалют) не выработано. Уголовная ответственность за преступления в области их оборота не установлена.

В Швейцарии, Финляндии и Мальте приняты соответствующие законы, создана правовая база позволяющая владеть и пользоваться виртуальными активами (криптовалютами) как финансовым активом и для владельцев криптовалютного бизнеса созданы максимально комфортные условия, что позволило привлечь значительные инвестиции. Более того, например, в Финляндии подготовлен и принят закон, регламентирующий контроль за деятельностью поставщиков криптовалютных услуг, в том числе криптовалютных бирж, провайдеров криптокошельков и эмитентов цифровых валют.

Похожая ситуация складывается в Канаде, Мексике, Австрии, Болгарии и Франции. Вместе с тем во Франции разрешено страховым компаниям использовать страховые продукты на базе вир-

[183] В США появился отдел киберфинансовых преступлений [Электронный ресурс] // Sciencepop, 2020. URL: http://sciencepop.ru/ (дата обращения: 01.02.2020).

туальных цифровых активов (Закон «О плане действий для роста и трансформации предприятий»).

В Китае (КНР) до тех пор государство, с момента использования виртуальных валют не проявило никакой правовой реакции. При этом в ее развитии правительство страны видело только риски распространения таких преступлений, как отмывание преступных доходов, сбыт наркотических средств, взяточничество. Затем ситуация стала меняться. Уже в 2016 году появилась информация о том, что будет создана собственная виртуальная валюта (криптовалюта), которая в 2017 г. получила правовой статус объекта гражданских прав.

С 2017 года на уровне государства криптобиржам стали предъявляться определенные требования и биржевой оборот виртуальных активов (криптовалют) с момента введения в действие вышеупомянутого нормативно-правового акта стал строго контролироваться финансовыми институтами Китая.

Япония, как и множество стран прошла путь от отсутствия какого-либо регулирования оборота виртуальных активов (криптовалют) до понимания необходимости государственно-правового обеспечения этих процессов. В соответствии с законодательством Японии 2017 г. виртуальный актив признается как товаром, так и законным способом оплаты. Таким образом, данное государство интегрировало виртуальные активы (криптовалюты) в систему банковских расчетов между физическими лицами и организациями. В то же время она не является денежной единицей Японии, а имеет статус приравненный к фиатной валюте. Вышеуказанный статус позволяет ей выступать предметом множества гражданско-правовых сделок. Она может не только покупаться и продаваться, но и использоваться в качестве займа, быть расчетным средством, применяться в качестве задатка и неустойки, быть предметом конвертации, иметь курс обмена и т. д.

Сделки с виртуальными активами (криптовалютами) между частными лицами не запрещены и могут совершаться без ограничений. В то же время к деятельности организаторов торгов, несмотря на достаточно либеральный подход к заключению самих сделок применяются определенные требования. Так, предусмотрена обязательная регистрация любых криптоплощадок в Агентстве финансовых услуг Японии (FSA) и последующая ему подотчетность. Криптобиржа должна иметь резервный фонд в сумме эквивалентной 100 000 долларам США и систематически проводить аудит в налоговых органах. Соискателями лицензии могут быть только компании-резиденты Японии. Чтобы запустить процесс получения

лицензии, криптобирже необходимо заплатить государственную пошлину в сумме эквивалентной 300 000 долларам США. До введения Закона Японии 2017 года виртуальная валюта облагалась налогом на добавленную стоимость (НДС). С момента введения вышеуказанного закона этот налог отменен. В то же время налог на доход, полученный от продажи или прироста капитализации виртуальных активов (криптовалюты) в Японии, существует.

Южная Корея прославилась строгим подходом к криптоиндустрии. Она запретила во второй половине 2017 г. проведение ICO. В 2018 г. при активном участии Министерства экономики и финансов проведена комплексная проверка местных биткоин-бирж. В ходе проверки 14 бирж были признаны несостоятельными в связи с тем, что они оказались с низким уровнем кибербезопасности.

Подводя итог, следует отметить, что правовой статус виртуальных активов (криптовалюты) в большинстве государств мира не определен и несмотря на тот факт, что виртуальные активы (криптовалюты) не признаны законным платежным средством, но являются биржевым активом, они могут быть использованы в качестве платежного средства, средства обмена, мены и дарения. В большинстве государств предпринимаются меры по противодействию преступлениям, совершаемым с использованием виртуальных активов (криптовалют) или в отношении них. Имеющаяся правовая база в сфере киберпространства и противодействия киберпреступности в полной мере не отвечает современным требованиям и требует консолидации мирового сообщества к принятию единых правил игры как в повседневном использовании виртуальных активов (криптовалют), так и в противодействии преступлениям, с ее криминальным оборотом.

11.2. Легализация и проблемы правового регулирования оборота виртуальных активов (криптовалюты) в России и криминологические риски[184]

Стремительное развитие цифровых технологий, кажущиеся воплощением научной фантастики, привели к проблемам правового характера, которые на законодательном уровне пока не решены. И неслучайно после длительных изучений мнений о плюсах и минусах использования криптоиндустрии в России, основанной на принципах криптографии в среде распределенных реестров (майнинга), в октябре 2017 г. Президент Российской Федерации В. В. Путин поручил правительству и Банку России до 1 июля 2018 г. обеспечить внесение изменений в российское законодательство. Такие поправки законодательства должны включать регулирование производства виртуальных активов (криптовалют) и публичного привлечения денежных средств и виртуальных активов (криптовалют) путем размещения токенов по аналогии с регулированием первичного размещения ценных бумаг и разработать порядок налогообложения и регистрации компаний, занимающихся добычей виртуальных активов (криптовалют) (майнингом)[185].

Для того, чтобы разобраться в этом вопросе рассмотрим проблемные вопросы легализации виртуальных активов (криптовалют) в России, выделив как ее положительные, так и отрицательные факторы.

Обратим внимание на положительные факторы легализации виртуальных активов (криптовалют). В основе любого вида виртуальной валюты лежит блокчейн технология, которая выходит далеко за рамки только выпуска виртуальных валют, но и занимает заметное положение в мировой финансовой системе.

Ее преимуществами является децентрализация, прозрачность, конфиденциальность, надежность и компромисс. Применение ее в государственном управлении и экономике позволит создать массу предпосылок для активного развития страны в целом, так, например, технологии распределенного реестра в потенциале

[184] В тексте использовались материалы статьи Т. В. Пинкевич «Легализация криптовалюты в России: за и против», опубликованной в сборнике статей по материалам V Международной научно-практической конференции: 3 ноября 2017 г. «Уголовная политика и правоприменительная практика // Северо-Западный филиал ФГБОУВО «Российский государственный университет правосудия» / отв. ред. д-ра юрид. наук, доц. Е. Н. Рахманова. Санкт-Петербург: ИД «Петрополис», 2017.

[185] URL: http://www.kremlin.ru/acts/assignments/orders/55879; http://www.kremlin.ru/acts/assignments/orders/55899 (дата обращения: 06.12.2020).

могут помочь в сборе налогов, распределении пособий и пенсий, ведении земельного кадастра, регистрации и оформлении документов мигрантов, выдаче паспортов, водительских удостоверений, использоваться таких сферах, как здравоохранение, недвижимость, страхование торговля и пр. Блокчейн может обеспечить целостность государственных записей и услуг, а также использована и как инструмент противодействия криминалу, поскольку его возможности позволят снизить уровень преступности в финансовой сфере и сделать невозможным распространение коррупции. Основными его характеристиками является: прозрачность данных, доверие – запись, внесенную в блокчейн изменить невозможно, отсутствие посредников – ведется запись и верификация без третьей стороны.

К положительным моментам внедрения блокчейн-системы можно также отнести возможность для прямого трансграничного инвестирования любых средств без комиссионных потерь на оператора и без страховых регулятивных сборов, что заставляет государственные экономические системы конкурировать перед каждым человеком и его экономическим потенциалом; они экономичны и осуществляются практически мгновенно.

Кроме того, внедрение блокчейн-технологий в практику позволит повысить прибыльность майнинга, деятельности по созданию новых структур (обычно речь идет о новых блоках в блокчейне) для обеспечения функционирования криптовалютных платформ. Аналогия с «добычей» вполне уместна, так как процесс «майнинга» биткойнов энергоемкий, поскольку требует больших вычислительных мощностей. Было рассчитано, что для генерации биткойнов требуется мощность свыше 1Гигаватта, что может быть сопоставимо с использованием электричества Ирландией. Стимулом для этого служит награда в виде двадцати пяти биткойнов, сложившему пазл, за каждый «блок». Любой, у кого есть доступ в интернет и вычислительные мощности для сборки криптографического пазла, может добавлять блоки в реестр. Таких людей называют «майнерами». На сегодняшний день имеются фермы по майненгу биткойна, литкойна, эфириума и др.

Виртуальные активы (криптовалюты) не привязаны ни к какой национальной валюте; регулируется рыночными отношениями, на ее курс влияют спрос и предложения; полностью автономна, отсутствует централизация; информация о транзакциях хранится на компьютере в зашифрованном виде у всех участников системы; пользователи системы могут задействовать видеокарты в собственных ПК для «добычи» виртуальных денег, а затем уже становятся игроками на криптовалютных биржах.

Количество видов виртуальных активов (криптовалют) ежегодно увеличивается и в настоящее время составляет более 1 000 видов, но первой такой валютой и самой популярной среди них стал биткоин (BitCoin), который и сейчас занимает лидирующее положение среди виртуальных валют. Он, как платежное средство, почти в 100 раз опережает другие популярные валюты такого рода (Bitcoin (BTC), Ethereum (ETH), Ripple (XRP), Litecoin (LTC), Bitcoin Cash (BCH), и др.).

В тоже время спрос на виртуальные активы (криптовалюты) велик, предложения о их реализации и инвестировании тоже не уступает спросу, что влияет на его курс. Так, только за последние три года неоднократно был взлет и падение курса криптовалют более чем на 1 200 % и, если в октябре 2016 г. он стоил около 1 000 долл., то 23 декабря 2017 г. его стоимость достигла 19 330 долл., а сегодня, по сравнению с декабрем 2017 г. произошло снижение и стоимость биткойна равна 8090 долл., в 2018 г. его курс падал до 2 560 долл. В настоящее время капитализация рынка биткоина составляет более $164 млрд, которые сосредоточены в руках всего лишь 7,11 % владельцев и рост составил 23 900 долл. По мнению специалистов, объем оборота в России уже достигает 1 % от ВВП. Она приобретается и продается, ими можно рассчитываться за товары и оказанные услуги. При этом форма оплаты может быть как виртуальной, так и натуральной. Их можно обменять на обычные деньги на финансовых площадках, которых сегодня уже множество.

Отрицательные факторы ее использования можно разделить на две группы: финансово-экономические и криминогенные.

Финансово-экономические факторы включают: не обеспеченность ликвидными активами и какими-либо гарантиями государственного либо частного капитала, поэтому они подвержены существенным курсовым колебаниям, в том числе спекулятивного характера, нет гарантии защиты прав потребителей финансовых услуг; отсутствие единого эмиссионного центра, осуществление операций на «виртуальных биржах» несет высокий риск потери стоимости виртуальных активов (криптовалют); они могут начать конкурировать с национальными деньгами и привести к их ослаблению.

Криминогенные факторы:

– отсутствие достаточной правовой основы для определения статуса виртуальных активов (криптовалют) и их регулирования, в том числе отсутствие юридических обязательств у субъектов отношений. В связи с этим правоохранительные органы не могут своевременно выявить нарушения и перекрыть своевременно платежный канал;

– анонимность проводимых платежей и неподконтрольность национальным органам власти. Финансовые, налоговые, судебные, правоохранительные и иные государственные органы, а также негосударственные или общественные организации не могут повлиять на транзакции участников названной платежной системы (отменить, заблокировать, оспорить или принудительно их совершить без доступа к приватному ключу владельца). Транзакция – это упорядоченная последовательность операторов обработки данных, которая переводит базу данных из одного согласованного состояния в другое. Это вызывает проблемы у правоприменителей, связанные с идентификацией лиц, причастных к противоправной деятельности.

Для России эта проблема болезненна, уже несколько лет вопрос легализации виртуальных активов (криптовалют) стоит на повестке дня перед ЦБ России и Правительством Российской Федерации. Можно проследить весь путь пробных шагов к ее исследованию и ее законодательному регулированию. В 2015 году Министерство Финансов Российской Федерации объявило биткойн, как вид криптовалюты денежным суррогатом, и предложило его запретить, а нарушителей привлекать к административной и уголовной ответственности. Данная позиция поверглась обоснованной критике. Очень сложно идет процесс определения статуса виртуального актива (криптовалюты).

В 2016 г. создается рабочая группа при Государственной Думе Российской Федерации. Цель – выработка единой согласованной позиции ведомств относительно оборота криптовалюты и подготовка проекта закона.

9 мая 2017 г. Указом Президента РФ утверждена Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы (9 мая 2017 г.). Для успешной ее реализации принят ряд нормативных актов, а также программа «Цифровая экономика Российской Федерации» (июнь 2017 г.) учрежден Международный Комитет цифровой экономики – платформа разработки и внедрения, проектов цифровой экономики, международное экспертное сообщество, проект поддержки Программы «Цифровая экономика Российской Федерации».

5 октября 2017 года на сочинском форуме инновационных финансовых технологий Finopolis руководитель Банка России Эльвира Набиуллина заявила о том, что использование криптовалют как законного платежного средства не будет легализовано, поскольку они являются частными цифровые деньги. Центральный Банк против частных денег, в какой бы форме они ни были – материальной или виртуальной.

11 октября 2017 г. Президент Российской Федерации В.В. Путин поручил правительству и Банку России до 1 июля 2018 г. обеспечить внесение изменений в российское законодательство. Такие поправки законодательства, по его мнению, должны включать регулирование производства виртуальной валюты (криптовалюты) и публичного привлечения денежных средств и виртуальных валют (криптовалют) путем размещения токенов и разработать порядок налогообложения и регистрации компаний, занимающихся их добычей (майнингом).

И несмотря на то что начиная с 2015 г. и по настоящее время нет согласованной позиции заинтересованных ведомств относительно оборота виртуальных активов (криптовалют), развитие их рынка и оборота, рост соответствующих транзакций с ее использованием ежедневно увеличивается. Существенное число таких транзакций и ICO осуществляются российскими гражданами и компаниями в иностранных юрисдикциях, обладающих благоприятным правовым режимом, что требует правового регулирования.

В настоящее время ряд федеральных законов уже принят[186], еще пакет документов находится на стадии обсуждения, но как подчеркивает в своем ответе FATF Росфинмониторинг (2019 г.): «в настоящее время в связи с совершением преступлений с использованием криптовалют, несмотря на неопределение их правового статуса в законодательстве России, по сути они фактически приравниваются к имуществу (в соответствии с целями использования криптовалют) и идентифицируются в денежном эквиваленте»[187].

Специальных ограничений оборотоспособности виртуальных активов (криптовалют) законодательство не содержало. Однако принятый в июле 2020 г. Федеральный закон «О цифровых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации»[188] содержит понятие цифровой валюты, но какая это валюта, то ли это цифровая валюта, которая будет российской и будет использоваться в российской информационной системе или это любая виртуальная валюта или это виртуальный актив, как это предлагал Международный Банк. Это один момент. Второй заключается в том, что в самом понятии

[186] О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации [Электронный ресурс]. URL: https://base.garant.ru/72198096/ (дата обращения: 17.02.2021).

[187] URL: http://www.fedsfm.ru/news/957 (дата обращения: 24.03.2019).

[188] О цифровых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации: федер. закон от 31 июля 2020 г. № 259-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

(ст. 3 Закона) предлагается ее использовать в качестве платежа. При этом под обращением цифровой валюты в Российской Федерации понимаются сделки и (или) операции, влекущие переход цифровой валюты от одного обладателя к другому, российским организациям, а также филиалам, представительствам и иным обособленным подразделениям международных и иностранных 18 организаций, созданных на территории Российской Федерации, а также физическим лицам, фактически находящимся в Российской Федерации не менее 183 дней в течение 12 следующих подряд месяцев, запрещено принимать ее в оплату за товары (работы, услуги) (п. 5 ст. 14 Закона).

В гражданском обороте цифровая валюта фактически признается средством сбережения капитала. Ее можно продать, обменять или подарить; оплата цифровой валютой возможна только в пределах иностранных юрисдикций. Однако для использования цифровой валюты в гражданском обороте требуется ее декларирование, а при его отсутствии она не подлежит судебной защите.

Уголовное законодательство не содержит специальных норм, устанавливающих уголовную ответственность за нарушение имущественных отношений, связанных с оборотом виртуальных активов (криптовалют). В то же время Министерством финансов РФ подготовлен законопроект «О внесении изменений в статью 14 Федерального закона «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации», в котором содержатся предложения о привлечении к уголовной ответственности за организацию незаконного оборота цифровых прав и организацию незаконного оборота цифровой валюты. Более реальные предложения по совершенствованию уголовного закона в данной сфере были даны МВД России, в их числе дополнение ст. 63 УК РФ, где использование цифровой валюты в преступных целях, является отягчающим обстоятельством и дополнение примечания к ст. 158 УК РФ в части определения виртуальных активов (криптовалюты) в качестве имущества.

Рассматривая криминологические риски развития цифровых технологий и использования и распространения виртуальных активов (криптовалют), следует отметить, что согласно проведенному журналом ForkLog[189] интернет-опросу 3 000 человек в конце 2017 г. обладателей виртуальных валют (криптовалют). Среди опрошен-

[189] Итоги опроса «Биткоин и другие криптовалюты в нашей жизни» [Электронный ресурс]. URL: https://forklog.com/itogi-oprosa-forklog-bitkoin-i-drugie-kriptovalyuty-v-nashej-zhizni/ (дата обращения: 13.01.2019).

ных оказалось 90,2 %, при этом планируют их приобрести 6,6 %; 40,3 % респондентов хранят в них до 1 тыс. долл.; примерно 29,7 % – от 1 до 5 тыс.; 10,8% – до 10 тыс.; 12,4% – от 10 до 50 тыс.; 2,3 % – до 100 тыс. долл. 48 % опрошенных отметили, что доверяют криптобиржам; 40 % – не доверяют, но вынуждены пользоваться.

Что касается ICO (участие в торгах на криптовалютных биржах), то 43,6 % опрошенных в них не участвовали и не собираются; 32,1% планируют; 21,2 % принимали участие уже несколько раз; 3,1 % – множество раз.

Более половины опрошенных (50,5 %) считают биткоин глобальной валютой будущего; 27,6 % – многофункциональным цифровым товаром; 19 % – спекулятивным активом, который не имеет значимого практического применения; а 2,8 % видят в нем лишь предмет коллекционирования.

Таким образом, данные показывают, что виртуальные активы (криптовалюты) не только воспринимаются обществом в качестве валюты, но и превращаются в инвестиции. Криптовалютная деятельность масштабно развивается, и, если государство сможет оптимизировать экономические процессы, то криптовалюты и технология блокчейн смогут обеспечить существенный прирост ВВП[190], с одной стороны, а с другой нагрузка на правоохранительные органы увеличится в связи с ростом преступлений, совершаемых в этой сфере.

Изучение судебной практики уголовных дел и отказных материалов свидетельствуют о том, что количественные и качественные показатели зарегистрированных преступлений свидетельствуют о высоком уровне распространения деяний, совершаемых как в отношении виртуальной валюты (криптовалюты), так и с ее использованием. При этом, уровень латентности таких преступлений высок, поскольку отсутствие законодательной базы, понятийного аппарата, методических рекомендаций по расследованию такого рода преступлений, высокий уровень виктимизации населения, приводит к тому, что большая часть обращений населения о совершении в отношении их имущества (криптовалюты) преступлений остается без внимания правоохранительных органов. Усугубляется ситуация еще и тем, что большая часть населения, не имея правовой подготовки, порой не знает как защитить свои интересы и не обращается в правоохранительные органы.

---

[190] *Долгиева М.М.* Социальная обусловленность возникновения уголовно-правовых запретов нарушений, совершаемых в сфере оборота криптовалюты // Актуальные проблемы российского права. 2018. № 10.

Между тем, у исследуемых преступлений высокая степень общественной опасности, которая подтверждается ущербом, причиненным личности, обществу, государству, совершением деяния группой лиц по предварительному сговору, организованной группой, преступным сообществом, о чем свидетельствует судебная практика.

Особое место отведено преступлениям, совершаемым в финансово-кредитной сфере. Уже сегодня следует говорить о росте таких преступлений, как легализация (отмывания) денежных средств или иного имущества, приобретенных преступным путем, мошенничество и вымогательство, совершаемые с использованием виртуальных активов (криптовалют). Вымогательство как криминальный бизнес, о котором не раз предупреждали эксперты, получило уже высокий уровень распространенности во всем мире. При этом факты мошенничества в IT-сфере будут только увеличиваться. Так, два наглядных факта свидетельствуют о том, что эксперты говорят об этом без преувеличения, поскольку в мае и 27 июня 2017 г. серия вирусов-шифровальщиков WannaCry и Petya, да и позже уже неоднократно атаковали компьютерные системы по всему миру и вызвали операционные сбои как в цифровой, так и в операционной деятельности крупных международных и российских компаний. При этом, для разблокировки компьютерных систем преступники в качестве оплаты потребовали криптовалюту – биткойн.

Использование виртуальных активов (криптовалют) способствует расширению криминальных границ не только в экономической сфере. В последние годы участились случаи их использования при оплате: заказных преступлений, приобретении и распространении порнографических материалов, незаконно приобретенного оружия и боеприпасов, наркотических средств, психотропных и сильнодействующих веществ, а также при торговле людьми, организованную педофилию и незаконное изъятие, хранение, транспортировку и использование органов и тканей человека для трансплантации, финансирование терроризма и экстремизма, и пр.

Сказанное приводит к выводу о том, что распространение противоправных деяний, связанных с оборотом виртуальных активов (криптовалют), с их использованием при совершении преступлений, в качестве средства платежа и т. п. в России очевидно. Очевиден и тот факт, что для противостояния распространению преступности необходимо, прежде всего, создание современной правовой основы. Однако отсутствие легального нормативного регулирования названного цифрового актива не позволяет противостоять его

использованию при совершении преступных деяний, что требует разработки уголовно-правового механизма противодействия преступлениям, совершаемым с ее использованием.

Контрольные вопросы

1. Дайте оценку криминологических рисков использования виртуальных валют (криптовалют) представителями организованных преступных формирований.

2. Определите причины и условия, способствующие преступной деятельности с использованием виртуальных валют (криптовалют).

3. Назовите международные организации, формирующие общие положения о противодействии преступной деятельности с использованием виртуальных валют (криптовалют)

4. Какое влияние оказывает законодательное регулирование на динамику преступлений, совершаемых с использованием виртуальных валют (криптовалют)?

Глава 12. Криминологическая характеристика экономической преступности в условиях цифровой трансформации

Планируемые результаты освоения темы главы

– **знать** основные виды современной экономической преступности, ее структуру, количественные показатели и детерминанты, структуру личности преступника, совершившего преступление в сфере цифровых технологий;

– **уметь** определять причины и условия, способствующие совершению преступлений экономического характера с использованием цифровых технологий на основе полученных знаний определять конкретные меры предупреждения рассматриваемых преступлений;

– **владеть** навыками определения криминологического анализа преступлений экономического характера, совершаемых с использованием цифровых технологий и составления планов ее предупреждения.

12.1. Современное состояние преступлений экономической цифровой преступности

С развитием современных технологий сформировались условия к появлению нового вида преступлений, совершаемых в цифровом пространстве (цифровых преступлений). Большинство из этих преступлений совершаются в экономической сфере и способны причинить реальный вред отношениям собственности и нормальному порядку осуществления предпринимательской или иной экономической деятельности. Размер причиняемого ущерба от преступлений экономического характера, совершаемых с использованием цифровых технологий, за последние годы многократно вырос. Ежегодные убытки мировой экономики от экономических преступлений, совершаемых в цифровом пространстве, составили более 600 миллиардов евро. Их особенность заключается в том, что они могут быть совершены как в материальном мире, так и в цифровом пространстве. Они обладают своей спецификой и, следовательно, их можно выделить в отдельную категорию. Такие преступления могут быть направлены на отношения, складывающиеся в сфере нормаль-

ного оборота компьютерной информации; собственности; в сфере экономической деятельности и т. д.

Родовым объектом экономических преступлений, совершаемых в цифровом пространстве, следует признать экономические отношения, обеспечивающие материальное благосостояние личности, общества и государства, поскольку на них направлено общественно опасное деяние и именно им причиняется вред в первую очередь. Видовым объектом, в зависимости от конкретного состава, могут выступать отношения собственности (ст.ст. 159, 159.6, 160, 163 УК РФ), отношения в сфере экономической деятельности (ст.ст. 171, 171.2, 172, 183 УК РФ и др.). В зависимости от способа совершения преступления дополнительным объектом может выступать совокупность общественных отношений по правомерному и безопасному использованию компьютерной информации, а также общественная безопасность и общественный порядок.

На основании вышеизложенного можно привести следующую классификацию экономических преступлений, совершаемых в цифровом пространстве по видовому объекту посягательства:

a) цифровые преступления против собственности:

– хищения – мошенничество (ст. 159 УК РФ), мошенничество в сфере кредитования (ст. 159.1 УК РФ); мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ), присвоение и растрата (ст. 160 УК РФ);

– иные преступления против собственности – вымогательство (ст. 163 УК РФ), причинение имущественного ущерба путем обмана и злоупотребления доверием (ст. 165 УК РФ), умышленное уничтожение или повреждение чужого имущества (с. 167 УК РФ);

b) цифровые преступления в сфере экономической деятельности:

– преступления против интересов предпринимательства – незаконное предпринимательство (ст. 171 УК РФ); незаконные организация и проведение азартных игр (ст. 171.2 УК РФ); незаконная банковская деятельность (ст. 172 УК РФ); незаконное получение кредита (ст. 176 УК РФ); легализация (отмывание) денежных средств или иного имущества, полученных преступным путем (ст. ст. 174, 174.1 УК РФ);

– преступления против свободной и добросовестной конкуренции – принуждение к совершению сделки или к отказу от ее совершения (ст. 179 УК РФ); незаконное использование средств индивидуализации товаров, работ и услуг (ст. 180 УК РФ); незаконное получение и разглашение сведений, составляющих коммерческую,

налоговую или банковскую тайну (ст. 183 УК РФ); неправомерное использование инсайдерской информации (ст. 185.6 УК РФ);

– иные преступления в сфере экономической деятельности – фальсификация Единого государственного реестра юридических лиц, Реестра владельцев ценных бумаг или системы депозитарного учета (ст. 170.1 УК РФ); манипулирование рынком (ст. 185.3 УК РФ); совершение валютных операций по переводу денежных средств в иностранной валюте или валюте Российской Федерации на счета нерезидентов с использованием подложных документов (ст. 193.1 УК РФ); сокрытие денежных средств либо имущества организации или индивидуального предпринимателя, за счет которых должно производиться взыскание налогов и (или) сборов (ст. 193.2 УК РФ); фиктивное банкротство (ст. 197 УК РФ); уклонение от уплаты налогов и (или) сборов с физического лица (ст. 198 УК РФ); уклонение от уплаты налогов и (или) сборов с организации (ст. 199 УК РФ).

В цифровом пространстве существует реальная возможность совершения двух групп цифровых преступлений экономического характера, в основе которых объект или способ совершения преступлений. Так, в зависимости от способа совершения эти преступления можно разделить на:

– преступления с использованием психологического воздействия на человека (обман, введение в заблуждение, угрозы);

– преступления, совершаемые путем воздействия и использования цифрового оборудования (компьютеры, смартфоны, маршрутизаторы и иное оборудование).

Такое деление обусловлено, прежде всего тем, что в первую группу этих преступлений входят такие общественно опасные деяния, при совершении которых причиняется вред только лишь основному непосредственному объекту – экономическим отношениям. При совершении преступлений второй группы преступник причиняет вред как основному (экономическим отношениям), так и дополнительному объекту – отношениям, по правомерному и безопасному использованию компьютерной информации.

Цифровые преступления первой группы отличаются тем, что при их совершении преступники в своих целях используют уже существующие сайты, форумы и готовое программное обеспечение. Им нет необходимости совершать неправомерный доступ к компьютерной информации, они работают с тем, что им предоставляет цифровое пространство само по себе.

К таковым преступлениям можно отнести основной состав мошенничества (ст. 159 УК РФ), вымогательство (ст. 163 УК РФ),

причинение имущественного ущерба путем обмана и злоупотребления доверием (ст. 165 УК РФ), фальсификацию единого государственного реестра юридических лиц (ч. 1 ст. 170.1 УК РФ), незаконное предпринимательство (ст. 171 УК РФ), незаконное использование средств индивидуализации товаров, работ и услуг (ст. 180 УК РФ), незаконное разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну (ч. 2 ст. 183 УК РФ), и другие.

Способ совершения данных цифровых преступлений мало чем отличается от способа совершения аналогичных преступлений в материальном мире: при мошенничестве – обман либо злоупотребление доверием; при вымогательстве – угроза; при фальсификации – предоставление заведомо ложных данных и т. д. Обман в цифровом пространстве несет тот же характер общественной опасности, что и обман в материальном мире, однако теперь они осуществляются дистанционно, то же проявляется и с угрозами и с другими ранее оговоренными способами.

К преступлениям второй группы следует отнести мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ), внесение заведомо недостоверных сведений в реестр владельцев ценных бумаг либо систему депозитарного учета (ч. 2 ст. 170.1 УК РФ), незаконное получение сведений, составляющих коммерческую, налоговую или банковскую тайну (ч. 1 ст. 183 УК РФ), и др.

При совершении данных преступлений лицо может использовать специальные программы, позволяющие беспрепятственно осуществить неправомерный доступ к компьютерной информации, либо использовать вирусы, троянские программы, компьютерные черви и другие вредоносные программы. Используя данное вредоносное программное обеспечение при совершении экономических преступлений в цифровой среде, виновное лицо причиняет вред сразу двум объектам – экономическим отношениям и отношениям в сфере компьютерной информации.

Следовательно, под преступлениями экономического характера, совершаемыми с использованием цифровых технологий следует понимать преступления, совершаемые дистанционно, путем использования средств компьютерной техники, информационно-телекоммуникационных сетей, цифровых технологий и образованного ими цифрового пространства, имеющих родовым объектом экономические отношения.

Раскрывая особенности современного состояния преступлений экономического характера, совершаемых с использованием цифровых технологий, выясняется, что преступления имеют тенденцию к росту. Так, например, только за 2019 г. в этой сфере зарегистри-

ровано 294 тыс. преступлений, что на 70 % больше, чем в 2018 г. Из них 98, 4 тыс. зарегистрированных преступлений относится к категории тяжких и особо тяжких преступлений. Ущерб от хищений, совершенных с использованием цифровых технологий в 2019 г., по данным МВД России, составил более 10 млрд рублей[191], а раскрываемость этих преступлений составила 20,5 %[192].

Первая половина 2020 г. также ознаменовалась ростом преступлений с использованием информационно-телекоммуникационных технологий. Так, только за 5 месяцев этого года зарегистрировано 180,5 тыс. преступлений, совершенных с или на 85,1 % больше, чем за аналогичный период прошлого года, из них количество особо тяжких преступлений возросло на 66,3 % (16,7 тыс.), тяжких – на 141,9 % (76,5 тыс.). Большая часть из них совершена в финансовой и банковской сфере, против собственности как юридических, так и физических лиц и пр. Следует отметить высокий рост цифровых преступлений против собственности, включающие мошенничество, присвоение или растрата, вымогательство, причинение имущественного ущерба путем обмана и злоупотребления доверием и умышленное уничтожение или повреждение чужого имущества.

Так, основную долю в данной группе занимают деяния предусмотренные ст. 159 УК РФ (Мошенничество). И несмотря на то что в таблице № 1 представлена статистика по всем зафиксированным фактам мошенничеств, их доля в деяниях, совершенных в цифровой среде велика. Больше половины цифровых преступлений «против собственности совершается с использованием сети Интернет (102,2 тыс. – рост на 74,1 % по сравнению с АППГ), значительная часть – с помощью мобильных телефонов (76,6 тыс. – рост на 99,7 % по сравнению с АППГ). Более двух третей преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, приходится всего на два состава – кражу и мошенничество»[193]. Рост краж, только за январь–май 2020 г. составил 158,2 %, по сравнению с аналогичным периодом 2019 г. Особое место занимает мошенничество, совершенное в сфере компьютерной информации (ст. 159.6 УК РФ), мошенничество с использованием электронных средств

[191] Обзор: МВД: ущерб от киберпреступлений в России превысил 210 млрд рублей [Электронный ресурс]. URL: forklog.com (дата обращения 17. 02.2020 г.).

[192] Краткая характеристика состояния преступности в Российской федерации за январь–декабрь 2019 года. МВД России (дата обращения 17.02.2020 г.).

[193] Аналитический материал «Состояние преступности на территории Российской Федерации в условиях пандемии COVID-19 и тенденция ее развития до конца 2020 года // ВНИИ МВД России, Академия управления МВД России, 2020.

платежа (ст. 159.4 УК РФ), рост которых только за первое полугодие 2020 г. составил 138,8 %. В связи с чем необходимо отметить, что «цифровые мошенничества» совершаются в 67 % случаев и их доля в числе всех мошенничеств постоянно увеличивается[194].

Таблица № 1

Ст. УК РФ	Кол-во зарег. прест. в 2018	Кол-во зарег. прест. в 2019	Кол-во зарег. прест. в 2020 (6 мес)
159	192 040	219 021	133 780
159.1	7 383	7 779	3 744
159.3	4 917	18 133	14 552
159.6	970	687	305
160	15 452	15 324	7 994

Такое преступление, как вымогательство, в последнее время переживает новый виток своего развития благодаря цифровому пространству. Цифровые вымогатели действуют в разнообразных вариантах получения незаконной прибыли, начиная от отказа в обслуживании по важным направлениям деятельности различных учреждений и заканчивая выкладкой конфиденциальной информации (зачастую интимного характера), но все эти ухищрения содержат одно – требование оплаты за совершение (разблокировку сайта) или несовершение (не выкладку интимных фото) действий. Точное число доли цифровых вымогательств в доли всех вымогательств статистикой не определено, однако можем предположить, что их доля достигает 80 %.

Таблица № 2

Ст. УК РФ	Кол-во зарег. прест. в 2018	Кол-во зарег. прест. в 2019	Кол-во зарег. прест. в 2020 (6 мес)
163	5 100	5 384	2 834
165	821	744	506

[194] Состояние преступности в России за январь – июль 2020 года / ГУ правовой статистики и информационных технологий.

После крупномасштабной компании государства, направленной на ликвидацию игровых заведений на территории России цифровое пространство (Интернет), дало возможность активизировать незаконную деятельность игровых казино. Данный бизнес приносит колоссальные доходы и не удивительно, что он воспользовался возможностями цифрового пространство. Доля таких зарегистрированных преступлений в общей структуре рассматриваемой группы составляет 64 %.

Не удивительно, что значительную долю в рассматриваемой группе преступлений составляют именно деяния, относящиеся к ст. 180 УК РФ. Перенос отношений в области купли-продажи в цифровой мир является трендом настоящего времени, это обусловлено экономической выгодой такой торговли. Колоссальный объем продажи через интернет позволил преступному миру воспользоваться этими процессами и для увеличения прибыли нелегально использовать чужой товарный знак.

Предмет цифровых преступлений может отличаться от предмета аналогичных преступлений, совершаемых в материальном мире, и иметь свои особенности. Поскольку цифровое пространство является некой виртуальной реальностью, то такие общественно опасные деяния, как, например, хищения (ст.ст. 159, 159.6, 160 УК РФ), не могут быть направлены на изъятие конкретных материальных предметов (бумажник, телефон, автомобиль), поскольку они существуют в цифровом пространстве. Однако данные преступления могут быть направлены на другие предметы, обладающие такой же экономической значимостью, существование которых возможно в цифровой среде (безналичные и электронные денежные средства, криптовалюта). В то же время цифровое пространство дает доступ к таким материальным предметам, как компьютер, планшет или смартфон, которые при определенных навыках можно умышленно повредить или вовсе уничтожить (ст. 167 УК РФ).

Электронные деньги обладают экономической и юридической значимостью, однако их нельзя потрогать, поскольку они лишены какого-либо материального выражения – это лишь денежное обязательство, запись о котором хранится в электронной форме. В связи с этим совершить кражу электронных денег нельзя, поскольку их физически невозможно изъять, однако их можно обратить. При этом причиняется реальный ущерб отношениям собственности, а значит, электронные деньги могут быть предметом хищения (основной состав мошенничества, мошенничества в сфере компьютерной информации, присвоения либо растраты).

Следовательно, такой признак предмета хищения, как материальность, в цифровом пространстве становится весьма условным. Цифровое пространство a priori не материально и любой предмет внутри него также материальным быть не может. Электронные деньги, с технической точки зрения, – это лишь совокупность нулей и единиц, однако именно они дают их обладателю имущественные права (цифровые права)[195], они могут принадлежать гражданину, организации или государству и могут приниматься как средство платежа в Российской Федерации и множестве других стран.

Отличительной особенностью всех цифровых преступлений является дистанционный способ их совершения. Такие преступления принципиально отличаются отсутствием физического или пространственного контакта между виновным и потерпевшим. Преступник может совершить хищение из банка, расположенного в другой стране, не выходя из дома, только с использованием цифрового пространства.

Дистанционное совершение преступления не снижает его общественной опасности. Представляется, что такой способ, наоборот, предполагает более серьезный подход к планированию и реализации преступного умысла. Так, для того, чтобы совершить, например, мошенничество путем обмана или злоупотребления доверием, преступник может зарегистрироваться в нескольких социальных сетях под разными именами и в течение продолжительного времени вести общение с ничего не подозревающими потерпевшими, и только после того, как он полностью завладеет их доверием, попросить денег и обмануть.

Дистанционный способ совершения преступления позволяет не оставлять физических следов, что затрудняет процесс доказывания и выявления преступника. Все что остается после совершения большинства цифровых преступлений – это записи на компьютере потерпевшего и записи его Интернет-провайдера. Единственное, что таким образом можно выявить, – это IP-адрес.

Также дистанционный способ совершения преступления позволяет преступникам оставаться анонимными и субъективно чувствовать себя защищенными от правоохранительных органов. Потерпевшие не могут описать ни примерный возраст, ни рост, ни пол преступника.

---

[195] О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации: федер. закон от 31 июля 2020 г. № 259-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс». Ст. 1.

12.2. Причинный комплекс и предупреждение экономической цифровой преступности

Результаты анализа исследования причинного комплекса, определение особенности преступного поведения личности преступника как основного звена механизма преступного поведения, необходимо для повышения эффективности предупреждения как в целом преступности, так и отдельных ее видов. По мнению Т. В. Пинкевич, «Экономическая преступность, как и преступность в целом, обусловлена сложным взаимодействием различных социальных факторов, находящихся в различных сферах и на различных уровнях жизнедеятельности общества, поэтому снизить уровень экономической преступности можно, только одновременно снижая уровень детерминант, ее порождающих, но решению этих проблем должно способствовать предупреждение экономической преступности»[196].

Известно, что все детерминанты преступности, в том числе и экономической цифровой преступности, носят как объективный, так и субъективный характер и классифицируют по содержанию: социально-политические, социально-экономические, правовые и идеологические. Такая классификация детерминант экономической преступности «позволит объяснить происхождение, процессы, порождающие преступность, установить факт связи между причиной и следствием и использовать полученные данные в ходе подготовки предупредительных мер»[197].

Все детерминанты экономической цифровой преступности можно также разделить на:

– общие детерминанты экономической преступности – это совокупность причин и условий, характерных как для экономической цифровой преступности, так и для всей экономической преступности в целом;

– специальные детерминанты экономической цифровой преступности – это совокупность причин и условий, характерных лишь для экономической цифровой преступности.

Следует уделить особое внимание специальным детерминантам экономической цифровой преступности, которые обусловлены, в первую очередь, особенностями цифрового пространства и информационно-телекоммуникационных технологий. Использование возможностей цифрового пространства облегчает процесс совершения

[196] Сборник избранных лекций по криминологии / под ред. д-ра юрид. наук, профессора Т. В. Пинкевич. Москва: Юрлитинформ, 2020.

[197] *Там же.*

преступления на каждом этапе, позволяет оставаться анонимным и не привлекать к себе лишнее внимание со стороны правоохранительных органов, снижает риск быть пойманным. К таковым следует отнести:

– анонимность цифрового пространства, информационно-телекоммуникационных сетей и самих пользователей цифрового пространства является одним из основных детерминант возникновения цифровой преступности. Если в материальном мире преступник скрывает свое лицо и прикладывает определенные усилия, чтобы не оставлять следов совершения преступления, то в цифровом пространстве это уже сделано за него;

– анонимность цифрового пространства – это основной принцип его существования. Все пользователи сайтов, форумов или социальных сетей в цифровом пространстве изначально не имеют ни имен, ни внешнего вида – они эфемерны, и нередко информационные ресурсы сами присваивают таким пользователям имя «anonymous», то есть аноним.

Следующий уровень анонимности – это сокрытие своих технических данных (IP-адрес, номер порта компьютера, потока данных и др.). Таким образом, создаются целые анонимные информационно-телекоммуникационные сети («TOP», «ANts P2P», «Freenet»).

Зарегистрировавшись под чужим именем, любой может безнаказанно обманывать, совершать анонимные платежи и переводы денежных средств, совершать хищения, вымогательства и иные экономические цифровые преступления.

Анонимность в цифровом пространстве является основным детерминантом цифровых преступлений и фактором высокого уровня латентности преступности в цифровом пространстве. Представляется, что наиболее эффективной мерой противодействия данной проблеме является персонализация доступа в цифровое пространство путем развития и внедрения биометрических технологий (сканера отпечатка пальцев, сканера лица пользователя).

Несовершенство законодательства создает условия для существования цифровой преступности. Отечественный законодатель часто не успевает ответить на новые вызовы цифровых преступников. Скорость развития цифрового пространства и скорость, с которой появляются новые способы совершения преступлений, превышает скорость реагирования на них со стороны государства.

Пробелы отечественного законодательства в области противодействия цифровой преступности создают условия для ухода виновных от ответственности, формируя тем самым чувство безнаказан-

ности за содеянное, которое и побуждает хакеров на совершение все новых преступлений.

Экстерриториальность цифрового пространства является важным детерминантом существования экономических цифровых преступлений. Преступления, совершаемые с использованием сети Интернет, нередко подпадают под несколько юрисдикций благодаря ее глобальной и межгосударственной природе.

Так, преступника и потерпевшего могут разделять от нескольких метров до нескольких тысяч километров, хотя в цифровом пространстве они могут быть постоянными посетителями одного и того же сайта или социальной сети. В то же время потерпевшие от одного цифровые преступления могут исчисляться десятками или сотнями, при этом они так же могут проживать в разных странах мира, как и сами преступники, если они действовали в соучастии. Субъективно виновный считает общественно незначимым такое деяние, как хищение электронных или безналичных денег у иностранца, или обман гражданина другой страны. Тот факт, что лицо совершает преступление против интересов иностранных граждан или организаций, субъективно снимает с него ответственность и развязывает руки. Цифровое пространство само по себе экстерриториально – в нем нет границ, нет государств, но есть сайты, форумы и их пользователи иностранцы, которых можно обмануть или обокрасть.

Данная проблема сильно усложняет работу следствия, доказывание, процесс экстрадиции и порождает проблему криминализации деяния. Некоторые экономические преступления, совершаемые в цифровом пространстве в России, либо вовсе не криминализированы, либо являются административными правонарушениями. Возможна и обратная проблема: криминализированные в России общественно опасные деяния могут не являться таковыми в других странах.

Единственный путь решения данной проблемы заложен в международном сотрудничестве.

Возможность получения сверхприбыли при минимальных затратах в цифровом пространстве – одна из основных социально-экономических причин экономической цифровой преступности.

В сложившейся обстановке сокращения традиционных форм трудовой деятельности и диктующей необходимость перевода значительной части населения на удаленные формы работы, а также осознания возможности получения доходов в цифровом мире вынуждает общество получать специальные знания и активизировать свою деятельность в цифровом пространстве. Одни занимаются законной деятельностью, другие ищут легкий путь – преступ-

ный (организовывают сайты-казино, занимаются мошенничеством, вымогательством, взломом аккаунтов пользователей, хищениями либо торговлей вредоносными программами). Многие хакеры за несколько дней становятся миллионерами.

Учитывая анонимность и трансграничность цифрового пространства, а также множество технических уязвимостей последнего, данное обстоятельство может являться катализатором, побуждающим к преступной деятельности отдельные группы населения.

Данную проблему, можно решить профилактикой цифровой преступности среди населения путем общей превенции уголовного закона.

Техническое несовершенство цифрового пространства. Техническое несовершенство цифрового пространства и наличие в нем технических уязвимостей, лазеек и просто ошибок сводит на нет почти все меры противодействия цифровой преступности.

Отсутствие цифровой культуры и грамотности. В цифровом пространстве отсутствуют как таковые правила поведения, поэтому многие администраторы сайтов или форумов вынуждены придумывать свои, при этом санкции, которые может наложить администрация, ограничены предупреждениями, ограничением доступа и блокированием доступа к ресурсу («бан»). Такие санкции являются малоэффективными, поскольку количество сходных сайтов в цифровом пространстве достаточно велико, и если на одном сайте нарушителя заблокируют, то он может свободно зарегистрироваться на другом, либо может заново зарегистрироваться на заблокированном сайте под другим именем. В этом плане более эффективна блокировка не пользователя, а его IP-адреса, однако и этот запрет можно обойти посредством специальных программ, либо осуществив доступ с другого устройства.

Единственным эффективным решением данной проблемы является профилактика информационной безопасности среди населения. Необходимо прививать основные правила поведения в цифровом пространстве с малых лет, например, проводя специальные занятия в средней школе.

Отсутствие единых и четких правил поведения в цифровом пространстве привело к появлению новых субкультур, таких как субкультура хакеров, киберпиратов и многих других.

Субкультура хакеров (взломщиков) также имеет значительное влияние на всю цифровую преступность – это своеобразное продвижение образа жизни и ценностей компьютерного преступника в широкие массы, реклама, делающая преступный путь привлекательным.

Общество не видит угрозы со стороны хакеров, считая их деятельность интересной и увлекательной. Данное мнение складывается у рядового пользователя цифрового пространства до тех пор, пока он не станет жертвой такого хакера. При этом занятие хакерством уже перестало быть неким развлечением, а является серьезным источником дохода.

Сложность выявления и квалификации деяний. Данный факт говорит о том, что многие сотрудники правоохранительных органов, впервые столкнувшиеся с цифровым преступлением, не обладают необходимыми знаниями, как по их квалификации, так и по поиску и привлечению к ответственности виновных, что приводит к высокому уровню латентности цифровой преступности.

Иллюзия незначительности ущерба для потерпевшего, по сравнению с проблемами, которые могут возникнуть при расследовании. Похожая причина существует и в том случае, если потерпевшим будет являться кредитная организация: расследование большинства видов цифровых мошенничеств затрудняется отсутствием необходимой информации о фактах совершения таких преступлений от кредитных организаций, так как многие банки, опасаясь за свою деловую репутацию, крайне неохотно обращаются за помощью в правоохранительные органы. Представители бизнеса часто утаивают факты хищений и кибер-атак, опасаясь причинения вреда своей репутации.

Следует уделить внимание и характеристике личности преступника, поскольку она является важной частью понимания самого явления цифровой преступности. Полученные данные помогут выделить примерный круг лиц, нуждающихся в дополнительном контроле со стороны государственных правоохранительных органов, что облегчит поиск виновных и предупреждение новых преступлений.

Построить примерный портрет компьютерного преступника пробовали многие отечественные исследователи, но единой точки зрения нет, что связано с разнородностью цифровой преступности. Однако почти все они так или иначе отдельно выделяют две самостоятельные группы цифровых преступников: хакеров и корыстных преступников. Нами будет проведен анализ именно корыстного цифрового преступника, поскольку подавляющее большинство экономических преступлений в сфере цифровых технологий – корыстной направленности.

Характеризуя социально-демографические признаки личности преступника, мы пришли к выводу, что в этой группе преступлений мужчины чаще совершают преступления (75 %), чем женщины, что свидетельствует о том, что мужчинам IT-технологии более знакомы, они в них лучше разбираются и по этой причине чаще совершают преступления. Как правило, большая часть этих преступле-

ний, совершают лица возрастной категории от 30 до 49 лет (52 %) и немного меньше второй возрастной категории 25–29 лет (18 %), имеющие высшее (27 %), средне – профессиональное (33 %), и среднее (полное) общее (28 %) образование. Как правила лица, совершившие эти преступления не состояли в браке (70 %) и не имели постоянного источника доходов (60 %), 17 % совершили эти преступления в составе преступных групп. 39 % от общего числа лиц, привлеченных к уголовной ответственности за экономические преступления, совершенные в сфере цифровых технологий, ранее уже привлекались к уголовной ответственности.

Почти все цифровые преступления, зафиксированные на территории Российской Федерации, были совершены из корыстных побуждений, мотив обогащения (98,4 %) и только 1,6 % в качестве основного – игровой мотив, но как свидетельствуют материалы практики и экспертные оценки, в некоторых случаях людьми движут и иные побуждения. Так, в условиях кризиса, находясь на грани увольнения, некоторые сотрудники посягают на информационные ресурсы корпорации и передают коммерческие секреты конкурентам не столько из корысти, сколько из соображений мести. Материальная выгода при этом имеет второстепенное значение.

Проведенный анализ позволил выделить два основных типа цифровых преступников:

Первый тип – лица, совершающие традиционные преступления (мошенничество, присвоение, растрату, вымогательство, незаконное использование товарного знака и другие) с использованием общедоступных ресурсов и возможностей цифрового пространства (таких как электронная почта или социальные сети) (традиционные цифровые преступники).

Второй тип – лица, совершающие экономические цифровые преступления (мошенничество в сфере компьютерной информации, незаконное собирание сведений, составляющих коммерческую, налоговую либо банковскую тайну, и др.) посредством неправомерного доступа к компьютерной информации либо с использованием вредоносного программного обеспечения в цифровом пространстве (вирусов, троянских программ, DDoS-программ и т. д.) (хакеры).

Данные типы цифровых преступников во многом отличаются друг от друга. Так, традиционные цифровые преступники, как правило, старше и опытнее хакеров – именно в данной группе цифровых преступников наибольшее число лиц, имеющих судимость. Хакеры, наоборот, как правило, моложе и являются выпускниками или учащимися высших учебных заведений технической направленности либо специальных техникумов и колледжей.

Цифровые преступники первого типа совершают традиционные преступления, то есть те, которые совершаются и без использования цифрового пространства (мошенничества, вымогательства, незаконное разглашение сведений, составляющих коммерческую тайну). Такие цифровые преступники при совершении преступлений не используют сложные вредоносные программы и вирусы, а пользуются возможностями цифрового пространства, которые есть в общем доступе: мошенничество путем обмана они совершают в социальных сетях, вымогательство – через электронную почту, а коммерческую тайну распространяют на форумах и т. д.

Цифровые преступники второго типа при совершении преступлений пользуются техническими уязвимостями цифрового пространства, взламывают электронные почтовые ящики, мобильные телефоны, банковские Онлайн-счета и электронные кошельки. Такие цифровые преступники хорошо разбираются в сложных компьютерных программах, знают принципы работы информационно-телекоммуникационных сетей и умеют пользоваться вирусами и иным вредоносным программным обеспечением.

Знания основных детерминант рассматриваемого вида преступлений и результаты исследования личности преступников, совершивших преступления в сфере цифровых технологий позволило меры противодействия этим преступлениям разделить на две основные группы: правовые и криминологические.

Правовые меры направлены на одно из основных условий экономической цифровой преступности – несовершенство законодательства. Они включают предложения по совершенствованию законодательства об уголовной ответственности за экономические преступления и преступления в сфере компьютерной информации; законодательства об информации, о связи и персональных данных. Правовые меры неразрывно связаны с организационными, поскольку они обеспечивают их исполнение на законодательном уровне. Без должного правового регулирования большинство организационных мер будут неэффективны.

Криминологические меры включают предложения по противодействию таким детерминантам экономической цифровой преступности, как анонимность преступников, экстерриториальность преступлений, отсутствие культуры цифровой безопасности у населения и наличие субкультуры хакеров. Криминологические меры содержат предложения по профилактике информационной безопасности среди отдельных групп населения, предложения по совершенствованию информационных технологий, а также предложе-

ния по квалификации экономических преступлений, совершаемых в цифровом пространстве.

Поскольку все экономические цифровые преступления по способу их совершения и объекту посягательства можно разделить на две самостоятельные группы (цифровые преступления, совершаемые путем воздействия на человека, и цифровые преступления, совершаемые путем воздействия на оборудование), то и меры противодействия экономическим цифровые преступлениям по объекту противодействия можно разделить на социальные и технические меры. Социальные меры направлены на развитие социальных качеств граждан (пользователей цифрового пространства): развитие культуры информационной безопасности и информационной грамотности, а также искоренение субкультуры хакеров. Социальные меры по способу противодействия также можно разделить на правовые и криминологические.

Многие преступления против собственности можно зафиксировать и предотвратить только с помощью специальных технических средств. При этом технические меры должны определяться в зависимости от характера и специфики защищаемого объекта и построения средств зашиты на основе высоких технологий. Технические меры направлены на развитие информационных технологий: разработку антивирусных программ, внедрение новейших информационных технологий в государственные и коммерческие организации, противодействие анонимности пользователей цифрового пространства и т. д.

Кроме того, представляется, что при подготовке сотрудников правоохранительных органов необходимо проводить специальные курсы о преступлениях, совершаемых в цифровом пространстве, а с действующими сотрудниками ежегодно проводить семинары о новых видах и новых способах совершения цифровых преступлений.

Контрольные вопросы

1. Назовите количественные и качественные характеристики экономической цифровой преступности.
2. Определите детерминанты экономической цифровой преступности.
3. Определите основные меры противодействия экономической цифровой преступности.
4. Определите тип и основные характеристики личности цифрового экономического преступника.

Глава 13. Криминологическая характеристика преступности в сфере интеллектуальной собственности в условиях цифровой трансформации

Планируемые результаты освоения темы главы

– **знать** особенности преступности в сфере интеллектуальной собственности в условиях развития цифровых технологий; понимать характерные ее особенности;

– **уметь** применять свои знания для понимания исследования закономерностей и тенденций развития преступности в сфере интеллектуальной собственности в условиях развития цифровых технологий; при анализе современного состояния этого вида преступности, использовать статистические показатели и выстраивать цепочку к изучению причин и условий, способствующих их совершению; ориентироваться в особенностях определения латентной преступности и социальных последствий;

– **владеть** терминологией преступности в сфере интеллектуальной собственности в условиях развития цифровых технологий; навыками для организации и проведения криминологических исследований; прогнозирования этого вида преступности, планирования профилактических мероприятий.

13.1. Современное состояние преступлений в сфере интеллектуальной собственности

Охране интеллектуальной собственности всегда уделялось особое внимание, поскольку любым новым открытиям и разработкам, направлениям в науке уделялось и уделяется особое внимание и не только государственными органами и частными кампаниями, но и криминальными структурами. Интеллектуальная собственность с развитием цифровых технологий приобрела особое значение, поскольку в построении цифровой экономики она играет решающую роль, став «ключевым правовым инструментом, опосредующим важнейшие экономические отношения, как право собственности в аграрную и индустриальную эпоху... большая часть стоимости IT–компаний заключается в их интеллектуальных активах»[198]. Предпочтение сегодня отдается тем направлениям, где продукты создаются благодаря творческому потен-

[198] *Близнец И. А.* Цифровые технологии и их влияние на развитие авторского прав и смежных прав. Авторское право в цифровую эпоху [Электронный ресурс]. URL: www1.fips.ru (дата обращения: 12.04.2021).

циалу человека и которые продолжают развиваться благодаря использованию интеллектуальной собственности. Это направление рассматривают как корпоративную индустрию. При этом следует отметить, что рынок интеллектуальной собственности за последние 5 лет вырос почти на 80 трлн долларов. С его развитием и значимостью, а также недостаточной правовой защитой новых технологий, увеличивается и количество посягательств на права интеллектуальной собственности. Известно, что интеллектуальная деятельность, интеллектуальный продукт, а также их виды раскрываются в качестве двух категорий:

1) «рынок интеллектуальных прав позволяет его участникам извлекать значительные доходы[199], ее следует рассматривать как категорию экономическую;

2) исключительные права на результаты интеллектуальной деятельности, которые следует рассматривать как юридическую категорию[200]. В данном случае владелец интеллектуальной собственности может ими распоряжаться и использовать по своему усмотрению, в том числе «передавать свои права на них другим лицам для использования, путем заключения договора-уступки, продавать свои права, запрещать третьим лицам совершать такие же действия без его (правообладателя) согласия»[201].

Объекты интеллектуальной собственности законодательно определены ч. 1 ст. 1225 ГК РФ, перечень которых включает: «произведения науки, литературы и искусства; программы для электронных вычислительных машин (программы для ЭВМ); базы данных; исполнения; фонограммы; сообщение в эфир или по кабелю радио- или телепередач (вещание организаций эфирного или кабельного вещания), изобретения, полезные модели; промышленные образцы; селекционные достижения; топологии интегральных микросхем; секреты производства (ноу-хау); фирменные наименования; товарные знаки и знаки обслуживания; географические указания; наименования мест происхождения товаров; коммерческие обозначения»[202].

Как видно из перечня названных объектов, к ним относятся охраняемые правом результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации юридических лиц, товаров,

---

[199] *Дозорцев В. А.* О мерах по развитию рынка интеллектуальных продуктов // Законодательство и экономика. 1978. № 7.

[200] *Мандрыко А. В.* Уголовно-правовые и криминологические меры противодействия преступности в сфере интеллектуальной собственности: дис. ... канд. юрид. наук. Москва, 2017.

[201] *Там же.*

[202] Гражданский кодекс Российской Федерации от 30 ноября 1994 г. Доступ из справ.-правовой системы «КонсультантПлюс».

работ, услуг и предприятий, включающие авторские и смежные права, патентные права (промышленная собственность), средства индивидуализации участников гражданского оборота, товаров и услуг.

При совершении посягательства на общественные отношения в сфере охраны интеллектуальной собственности, виновный может быть привлечен к уголовной ответственности по ст.ст. 146, 147, 180, 183 УК РФ.

Исследование статистических показателей количества зарегистрированных преступлений и лиц их совершивших за последние тринадцать лет свидетельствуют о том, что они ежегодно показывают снижение, за исключением 2020 г. (см. диаграмму 1).

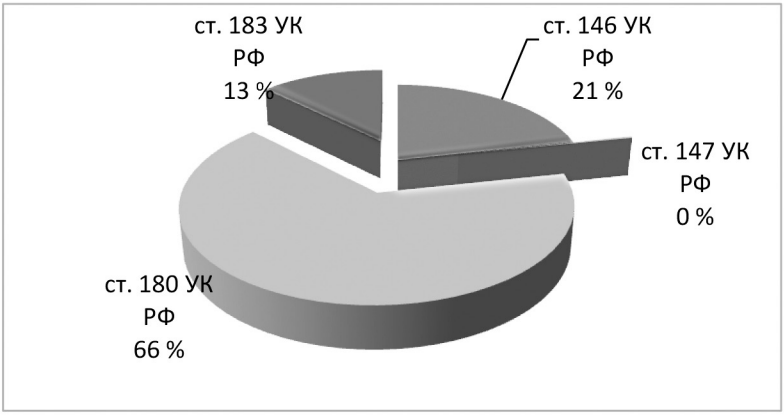
Диаграмма 1

Надо признать, что во второй половине 2000-х количество исследуемых преступлений стало меняться. Так, начиная с 2008 года количество зарегистрированных преступлений данного вида начинает снижаться, при этом небольшие всплески роста по отношению к предыдущему периоду прослеживаются в 2013, 2017 и 2019 г.г. Кроме того, судя по показаниям количества зарегистрированных преступлений этого вида в первом полугодии 2020 г. и сопоставление их с данными аналогичного периода 2019 г. этих с использованием цифровых технологий увеличивается и в ближайшие время прогнозируется рост этих преступлений. Вместе с тем следует отметить, что данный вид преступности имеет высокий уровень латентности. При изучении проведенных ранее исследований преступности в сфере интеллектуальной собственности и ее латентной части мы пришли к выводу о том, что в разные годы эти показате-

ли менялись. Так, например, поведенный А. Х. Гацолаевой анализ уровня латентности преступлений в сфере интеллектуальной собственности в 2004 г., по ее мнению, обладают средневысоким уровнем латентности[203]. Другие авторы, исследовавшие эту группу преступлений в 2016 г. относят ее к среднелатентным преступлениям[204]. Изучение этих преступлений в 2020 г. с уверенностью позволяет утверждать о высоком уровне латентности названных деяний.

Что касается структуры преступлений в сфере интеллектуальной собственности, то в проведенных ранее исследованиях указывалось, что «84 % совершено преступлений, предусмотренных ст. 146 УК РФ; 9 % приходится на долю ст. 180 УК РФ; 6,8 % – ст. 183 УК РФ; 0,2 % – ст. 147 УК РФ»[205]. Однако за последние годы ситуация изменилась кардинально. Так, по степени распространенности в этой группе на первое место можно поставить ст. 180 УК РФ (незаконное использование средств индивидуализации товаров (работ, услуг). Ее доля в группе этих преступлений достигла 66 %. Изменилась ситуация и с количеством зарегистрированных преступлений, предусмотренных ст. 146 УК РФ, на долю этой уголовно-правовой нормы приходится 21 % зарегистрированных преступлений. Возросло количество преступлений, предусмотренных ст. 183 УК РФ до 13 % (см. диаграмму 2).

Диаграмма 2



[203] См. *Гацолаева А. Х.* Криминологическая характеристика и предупреждение преступлений в сфере интеллектуальной собственности : автореф. дис. ... канд. юрид. наук : 12.00.08. 2004.

[204] *Мандрыко А. В.* Уголовно-правовые и криминологические меры противодействия преступности в сфере интеллектуальной собственности: дис... канд. юрид. наук. Москва, 2017.

[205] *Там же*.

Увеличение количества этих преступлений неслучайно, поскольку развитие и внедрение в повседневную жизнь общества цифровых технологий повысило, как представляется в первую очередь, уровень угроз обеспечения безопасности в сфере авторских прав, коммерческой и банковской тайны, персональных данных. Все чаще мы говорим о промышленном шпионаже как об одной из форм конкуренции, которая может применяется на всех уровнях экономики, а сейчас и цифровой экономики независимо от форм собственности предприятий, учреждений, организаций. Ее целью является незаконная добыча сведений, представляющих коммерческую ценность оперативными, техническими и цифровыми средствами. Цифровые средства в настоящее время стали ведущими в ведении промышленного шпионажа. И это не надуманная проблема, ущерб, причиняемый промышленным шпионажем государству, юридическим и частным лицам может быть колоссальным[206].

С целью выработки управленческих решений для повышения уровня конкурентной способности коммерческой деятельности названных предприятий осуществляется сбор и обработка данных из разных источников, но в рамках закона и соблюдения этических норм активно развивается конкурентная разведка. В современных условиях осуществляется путем контроля над глобальной телекоммуникационной сетью, платежными системами и коммуникациями, социальными сетями и электронными СМИ, корпоративными и локальными электронным системами, что позволяет в ходе разведки скрытно влиять на системы управления.

Действительно, с развитием ряда цифровых технологий увеличиваются угрозы расширения промышленного шпионажа, поскольку, например, технология распознания голоса, которая за несколько секунд может распознавать 10 000 образцов голосов с точностью до 90 %[207], используется преступниками с целью получения доступа в частные компании и промышленные предприятия. В том же направлении используется и система идентификации лиц.

Более интересен для преступников, совершающих преступления в сфере цифровых технологий, является перехват телекоммуникационного трафика. Особенно для них важна такая деятельность при подготовке к ряду иных преступлений с целью получе-

[206] Обзор: Промышленный шпионаж причинил полумиллиардный ущерб бюджету Свердловской области [Электронный ресурс]. URL: http://tvlesnoy.ru/promyshlennyj-shpionazh-prichinil-polumilliardnyj-ushherb-byudzhetu-sverdlovskoj-oblasti/ (дата обращения: 08.01.2021).

[207] Обзор: 7 самых современных шпионских технологий [Электронный ресурс]. URL: https://russian7.ru/post/7-samyx-sovremennyx-shpionskix-texnologij/ (дата обращения: 16.05.2020).

ния необходимой информации, которая позволяет им получать сведения о коммерческой и банковской тайне, о деятельности предприятий, которые готовятся, например, к недружелюбному поглощению и т. д.

В сфере интересов криминальных элементов выступает и технология «мобильный трекинг», позволяющая осуществлять слежения за деятельностью любых предприятий, организаций, учреждений и отдельных лиц. При этом он не отражается в телефоне как приложение, что позволяет длительное время не замечать слежения, а используя встроенный GPS телефона, программа слежения собирает координаты местонахождения мобильного телефона и через Интернет передает их на сервер слежения[208].

Следует также обратить внимание на то, что в последнее время большинство корпораций, предприятий и иных юридических лиц подвергаются хакерским атакам, в одних случаях их целью является мошенничество и вымогательство, в-других, вредоносный контент, в-третьих, хищение, получение информации, данных о деятельности юридических, а порой и физических лиц, а также пароли от аккаунтов и данные банковских операций. В этом случае используется такая технология, как кейлогеры, которые могут быть трех видов – программные (в виде скрытых программ на компьютере), аппаратные (встраиваются в сам компьютер или клавиатуру) и акустические (записывают и анализируют звуки клавиатуры и мыши).

Продолжает увеличиваться на потребительском рынке количество контрафактной продукции за счет незаконного использования товарных знаков, наименование места происхождения товаров и фирменных знаков.

Не исключен рост фальсифицированной и контрафактной продукции, многие эксперты считают, что увеличится количество некачественной продукции медицинского назначения, в том числе и неэффективные фальсификаты вакцины против COVID-19. Можно предположить, что они не только будут вкладывать значительные средства в их создание, но и распространять предложения на их приобретение с использованием цифровых технологий (Интернет, различные онлайн-платформы, социальные сети). В связи с экономическими проблемами у населения возможно повышение спроса на контрафактные товары, что будет влиять на расширение теневых рынков, развитие которых повлечет рост преступлений в сфере недобросовестной конкуренции и незакон-

[208] *Там же.*

ного использования интеллектуальной собственности[209]. Более того, известно, что «контрафактная продукция, являясь частью фальсифицированной продукции, представляет собой более общественно опасное явление, чем фальсифицированная продукция, не являющаяся контрафактной, поскольку помимо государственных интересов и интересов потребителей затрагивает еще права и интересы правообладателей»[210].

Нельзя не отметить, что изготовление и распространение контрафактной продукции, проведения мероприятий по промышленному шпионажу, по организации онлайн-торговли на несуществующих электронных площадках, создание видимости активной деятельности по защите интеллектуальной деятельности, с целью получения дополнительной информации о коммерческой тайне, причиняют существенный вред и повышают уровень криминогенности.

---

[209] *Пинкевич Т. В.* Экономическая преступность: современное состояние и прогноз // Уголовная политика и правоприменительная практика / Сб. статей по материалам VIII Международной научно-практической конференции 31 октября – 1 ноября 2020 г.: под ред. Е. Н. Рахмановой // Северо-Западный филиал ФГБОУ ВО РГУП, Санкт-Петербург. 2020.

[210] *Мандрыко А. В.* Уголовно-правовые и криминологические меры противодействия преступности в сфере интеллектуальной собственности: дис. ... канд. юрид. наук. Москва, 2017.

13.2. Причинный комплекс и предупреждение преступлений, совершаемых в сфере интеллектуальной собственности

Рассматривая причинный комплекс преступлений, совершаемых в сфере интеллектуальной собственности в условиях развития цифровых технологий, необходимо отметить, что потенциал любой страны зависит от уровня развития, прежде всего, инновационных технологий, в том числе и цифровых. С развитием цифровых технологий и повышением уровня информатизации общества интеллектуальная собственность, по мнению ряда авторов, стала основным цивилизационным драйвером развития, а институт интеллектуальной собственности – основой современной мировой экономики[211]. По данным проведенных исследований, сегодня свыше 70 процентов трафика в цифровых сетях приходится на движение объектов интеллектуальной собственности. Она стала не только значимым ресурсом экономики, но и инструментом развития цифровых технологий, формируя самостоятельный «цифровой рынок, рост которого превышает положительную динамику многих традиционных «материальных» товарных рынков. Все это определяет необходимость исследования развития института интеллектуальной собственности, его трансформации в условиях цифровизации экономики»[212].

В этих условиях интеллектуальная собственность становится «лакомым кусочком» для преступников, поскольку скорость, с которой внедряются цифровые технологии не имеет аналогов, с такой же быстротой создается и новая интеллектуальная продукция. В то же время механизмы защиты интеллектуальной собственности на этом уровне пока находятся только в стадии разработки. Между тем, учитывая тот факт, что совершаемые преступления в сфере интеллектуальной собственности с использованием цифровых технологий имеют свои, только ей присущие, уникальные характеристики, а именно, она не имеет географических границ, местом ее совершения является виртуальная среда, для совершения этих преступлений используются компьютерные данные, цифровые системы или социальные сети, поэтому предупреждение этого

[211] *Агамагомедова С. А.* Развитие института интеллектуальной собственности в условиях цифровизации экономики / С. А. Агамагомедова, Н. А. Надькина / Известия высших учебных заведений. Поволжский регион. Экономические науки. 2019. № 1 (9).

[212] *Там же.*

вида преступлений в настоящее время затруднено, так как развитие новой сферы требует подготовки организационно-управленческой правовой основы.

В настоящее время разработаны дорожные карты развития ряда сквозных технологий, приняты нормативные акты, способствующие их развитию. Внесены изменения в имеющиеся нормативные акты, но в тоже время не создана эффективная система управления интеллектуальной собственности. «Россия сегодня находится в начале процесса создания такой системы, которая позволит сформировать полноценный рынок интеллектуальной собственности и адаптировать законодательство к вызовам цифровой экономики»[213], не разработаны механизмы защиты цифровых технологий, методологические подходы к ее оценке, ее реализации в условиях цифровой экономики и контроля над этими процессами, это существенным образом влияет на характер и результаты использования цифровых технологий и на рост преступности. Следует отметить, что в рамках создания интеллектуального конкурентоспособного рынка действует Национальная интеллектуальная инициатива (IPNet) и ее стратегия активно внедряется в жизнь общества, разработана концепция «дорожной карты» IPNet с целью регулирования рынка интеллектуальной собственности для новой экономической реальности в интересах населения России. В рамках Инициативы создан Национальный координационный центр обработки транзакций с правами и объектами интеллектуальной собственности (IPChain), то есть на основе технологии блокчейн открыта общественная сетевая платформа для управления интеллектуальной собственностью, которая позволяет обладателю быстро зарегистрировать права на интеллектуальную собственность и способствует оперативному взаимодействию между участниками рынка интеллектуальной собственности, среди которых ключевую роль играют государственные структуры, с одной стороны, а с другой развитие цифрового рынка интеллектуальной собственности через создание сервисов правовой охраны, управления и защиты прав, позволит решить проблемы авторского, смежных и патентных прав. В настоящее время рассматривается вопрос на основе национальной сети IPChain «создание электронной биржи интеллектуальной собственности, где правообладатель сможет напрямую связаться с пользователем. Это также позволит расширить число участников сферы интеллектуальной

[213] Инновационное развитие и защита интеллектуальной собственности в цифровой экономике [Электронный ресурс]. ТАСС. URL: //https://tass.ru/pmef-2017/articles/4274740 (дата обращения: 18.10.2021).

собственности»[214]. Цифровая платформа позволит объединить юридическую поддержку, страхование, бухгалтерские или аудиторские услуги, и т. п.

В октябре 2018 г. утверждено адаптированное для Российской Федерации Типовое положение «Политика в области интеллектуальной собственности для университетов и научно-исследовательских организаций»[215], которое должно стать ориентиром в формировании политики данных организаций в области интеллектуальной собственности, раскрыть подходы к организации работы с ней, дать наглядное представление о ключевых элементах и этапах разработки политики данных организаций в области интеллектуальной собственности.

В это же время под эгидой Роскомнадзора подписан Меморандум о сотрудничестве в сфере охраны исключительных прав в эпоху развития цифровых технологий, согласно которому правообладатели создают реестр с указанием страниц сайтов с пиратским аудио- и видеоконтентом, а администраторы интернет-ресурсов обязаны ежедневно каждые пять минут обращаться к этому реестру и в течение шести часов удалять из поисковой выдачи ссылки на пиратские сайты в отношении объектов авторского права компаний, подписавших документ[216].

В 2020 г. в часть четвертую Гражданского кодекса РФ внесены изменения в части, касающейся изменения порядка регистрации интеллектуальной собственности, в том числе предоставления заявителю возможности прилагать к материалам заявки 3D модели заявляемых объектов интеллектуальной собственности (изобретений, полезных моделей, промышленных образцов и товарных знаков) в электронной форме. Это «позволит повысить привлекательность и комфорт регистрационной системы, сократить сроки и повысить качество экспертизы, снизить затраты по выдаче бумажных охранных документов»[217]. Предполагается, что данные измене-

[214] В «Сколково» представили Национальную интеллектуальную инициативу [Электронный ресурс]. URL: https://www.intermedia.ru/news/310167 (дата обращения: 25.03.2021).

[215] Минобрнауки России при участии Минкультуры России, Минэкономразвития России, Роспатента, Ассоциации IPChain, Федерации интеллектуальной собственности, Фонда «Сколково», Российского научно-исследовательского института экономики, политики и права в научно-технической сфере, Национального исследовательского центра «Высшая школа экономики», Университета ИТМО, Южного федерального университета и Всероссийского научно-исследовательского института авиационных материалов совместно с Всемирной организации интеллектуальной собственности.

[216] URL: https://www.rbc.ru/rbcfreenews/5bdaf5329a79475d77c8a003 (дата обращения: 24.02.2021).

[217] В Госдуме поддержан законопроект о расширении использования электронных технологий при регистрации объектов интеллектуальных прав [Электрон-

ния позволят снизить сроки государственной регистрации объектов интеллектуальных прав и позволят повысить качество проведения информационного поиска за счет расширения круга квалифицированных специалистов в различных областях науки и техники.

Одним из механизмов обеспечения деятельности предупредительного характера следует рассматривать проведение криминологической экспертизы принимаемых законодательных решений и иных нормативных актов, регулирующих сферу интеллектуальной собственности[218].

И, конечно же, особое значение должно быть уделено разработке и реализации мер организационного, нормативно-правового и методического характера в целях обеспечения экономической безопасности[219]. В их числе: соответствующая подготовка специалистов, техническая оснащенность правоохранительных органов новейшими технологиями цифрового мира, сотрудников правоохранительных органов и банковской сферы, разработка методических рекомендаций по противодействию современным вызовам преступности. Но самое главное необходимо привлечение современных специалистов, имеющих определенные знания в названной сфере.

Особое внимание должно быть уделено исследованию организационно-управленческих причин как одной из составляющих причинного комплекса преступности в сфере интеллектуальной собственности. Росту преступности в сфере интеллектуальной собственности способствуют слабая деятельность контролирующих органов, специализированных субъектов противодействия преступности в этой сфере, недостаточный уровень подготовки комплекта правовых документов, отсутствие методических рекомендаций по своевременному выявлению и пресечению преступной деятельности в современных условиях и результатов исследования личности современного преступника. Это обусловлено тем, что в современных условиях преступления совершаются с использованием цифровых технологий, а такой вид преступной деятельности чаще

ный ресурс]. URL: https://rospatent.gov.ru/ru/news/gd-o-rasshirenii-ispolzovaniya-ehlektronnyh-tekhnologij-pri-registracii-obektov-intellektualnyh-prav (дата обращения: 05.06.2020).

[218] *Шабанов Д. В.* Криминологическая обоснованность уголовного законодательства и практики его применения в сфере охраны собственности: дис. ... канд. юрид. наук: 12.00.08 / Шебанов Дмитрий Валерьевич. Краснодар, 2017.

[219] *Пинкевич Т. В.* Легализация криптоиндустрии: за и против // Уголовная политика и правоприменительная практика: сб. статей по материалам V Всероссийской научно-практической конференции 3 ноября 2017 г. / под ред. д-ра юрид. наук, доцента. Е Н. Рахмановой // Северо-Западный филиал ФГБОУ ВО РГУП, Санкт-Петербург, 2018.

всего требует знаний цифровых технологий и умений ими воспользоваться в преступных целях и обязательно скрыть следы своей преступной деятельности.

В ходе предупредительной деятельности особое внимание должно быть уделено факторам духовно-нравственного характера, поскольку в современном российском обществе имеет место быть не только высокий уровень правового и нравственного нигилизма, но и недоверие к проводимым политическим и общественным мероприятиям, связанными с требованиями и предписаниями законов и норм морали. Что же касается совершения деяний в отношении интеллектуальной собственности, то, как оказалось, в большей части граждане не всегда видят грань между существованием конкретного защищаемого права интеллектуальной собственности и правонарушением.

В связи со сложившейся криминогенной ситуации в сфере интеллектуальной собственности и принятием ряда нормативных документов, в том числе Указа Президента Российской Федерации от 7 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» и Основных направлений деятельности Правительства Российской Федерации на период до 2024 года, которые утверждены 29 сентября 2018 года Председателем Правительства Российской Федерации Д. А. Медведевым[220], направленных на увеличение оборота прав на интеллектуальную собственность, обеспечение ее конкурентной способности в мировом масштабе, важнейшим направлением государственной политики в сфере противодействия исследуемого вида преступности должны стать:

– подготовка специалистов не только в сфере IT-технологий, но и с образованием и получением знаний в сфере интеллектуальной, особенно тех подразделений, которые непосредственно осуществляют мероприятия по противодействию преступлениям в сфере интеллектуальной собственности, повышения их профессионализма. В этих целях разработка новых программ в сфере дополнительного профессионального образования;

– повышение эффективности деятельности правоохранительных органов в сфере защиты интересов правообладателей интел-

[220] О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года: указ Президента Российской Федерации от 7 мая 2018 г. № 204 (с изменениями и дополнениями). Доступ из информационно-правового портала «Гарант»; Основные направления деятельности Правительства Российской Федерации на период до 2024 года от 29 сентября 2018 г. Доступ из информационно-правового портала «Гарант».

лектуальной собственности. С этой целью необходима координация деятельности всех заинтересованных субъектов предупредительной деятельности по охране интеллектуальной собственности, общественных организаций правоохранительной направленности, но и большое значение имеет взаимодействие с международными организациями, поскольку использование интеллектуальной собственности в цифровом формате, порой противозаконное, не позволяет решать проблемы противодействия этим преступлениям только в рамках одного государства из-за их трансграничного характера.

Контрольные вопросы

1. Проанализируйте современное состояние преступности в сфере интеллектуальной собственности.
2. Назовите основные показатели преступности в сфере интеллектуальной собственности в России.
3. Какова специфика преступлений, совершаемых в сфере интеллектуальной собственности с использованием цифровых технологий?
4. Проанализируйте меры предупреждения преступлений, совершаемых в сфере интеллектуальной собственности с использованием цифровых технологий.

Глава 14. Криминологическая характеристика экстремизма и терроризма в условиях цифровой трансформации

Планируемые результаты освоения темы главы

– **знать** особенности экстремизма и терроризма, их виды и криминологические проблемы в условиях развития цифровых технологий;

– **уметь** применять свои знания в профессиональной деятельности; определять особенности криминологической характеристики личности экстремиста и террориста; использовать основные показатели преступности для оценки состояния названного вида преступности в стране;

– **владеть** навыками криминологической оценки нормативных актов; юридической терминологией в сфере предупреждения терроризма и экстремизма; навыками применения правил криминологического анализа.

14.1. Современное состояние экстремизма и терроризма

К одной из наиболее сложных и обсуждаемых проблем, вызывающих тревогу всего мирового сообщества, относятся экстремизм и терроризм. Многообразие форм его проявлений, значительное число террористических и экстремистских организаций действующих в мире и в России, транснациональный характер их деятельности, увеличение количества угроз внешнего и внутреннего характера свидетельствуют о том, что деятельность по противодействию им требует особого внимания, поскольку такие явления, особенно терроризм, продолжают представлять серьезную угрозу международной безопасности[221]. Это подтверждается статистическими данными, свидетельствующими о том, что только в 2015–2017 гг. в мире было совершено около 12 тыс. террористических актов, жертвами которых стали более 45 тыс. человек. При этом, более 30 тыс. человек погибло, среди них 81 % составляют жертвы терактов, около 36 тыс. человек получили ранения различной тяжести в результате названных деяний[222]. Атакам террористов

[221] *Овчинский В. С.* Иностранные боевики-террористы. Иногда они возвращаются. (Коллекция Изборского клуба). Москва: Книжный мир, 2019.

[222] Самые громкие теракты 2017 года [Электронный ресурс]. URL: https://versiya.info/mozaika/14832 (дата обращения: 31.10.2020); *Пинкевич Т. В.* Проблемы противодействия терроризму в условиях глобализации // Международно-право-

подверглись 92 страны, 55 % из которых были сосредоточены в Афганистане, Ираке, Пакистане, Индии и Нигерии[223]. В 2018–2019 гг. около 70 государств испытали на себе последствия более 5 тыс. резонансных террористических акций, от которых пострадало около 30 тыс. человек[224]. 2019 г. не стал исключением, по всему миру было совершено свыше двух тысяч террористических актов, в результате которых погибли и пострадали свыше 11 тыс. человек[225].

Сегодня особую тревогу во всем мире вызывает рост ненависти и ксенофобии, связанный с пандемией коронавируса. Так, по мнению Генерального секретаря ООН Антониу Гутерриша, распространение коронавирусной инфекции COVID-19 способствовало росту ненависти и ксенофобии, стали распространяться антисемитские теории заговора, призывы нападать на мусульман, мигрантов и беженцев, обвиняя их в том, что они являются источниками распространения этого заболевания. Он призвал политических лидеров проявлять солидарность с гражданами любых национальностей и укреплять социальную сплоченность[226].

Россия тоже не осталась в стороне. Согласно данным правоохранительных органов только в 2019 г. в России было зарегистрировано 1 806 преступлений террористического характера, предотвращено около 40 терактов, что позволило нейтрализовать 32 боевика, задержать – 679, а также ликвидировать 49 террористических ячеек, которые планировали атаки в различных регионах России[227]. Кро-

вые средства противодействия терроризму в условиях глобализации. Проблемы террористического наемничества среди молодежи и пути их преодоления: сб. материалов Всероссийской научно-прак. конф. Ставрополь: СГПИ, 2016; URL: http://ru.valdaiclub.com/a/highlights/terrorizm-vo-frantsii-v-2015-godu/ (дата обращения: 10.01.2020).

[223] URL: http://ru.valdaiclub.com/a/highlights/terrorizm-vo-frantsii-v-2015-godu/ (дата обращения: 16.03.2021); URL: http://ria.ru/society/20160419/1415127989.htm (дата обращения: 15.10.2017).

[224] Крупные теракты в мире в 2018 году: https://ria.ru/20180725/1525288381.html; Жертвами самых крупных терактов в 2019 году стали более 9 тысяч человек [Электронный ресурс]. URL: s://www.dp.ru/a/2019/10/13/ZHertvami_samih_krupnih_te (дата обращения: 16.04.2021).

[225] Жертвами самых крупных терактов в 2019 году стали более 9 тысяч человек [Электронный ресурс]. URL: s://www.dp.ru/a/2019/10/13/ZHertvami_samih_krupnih_te (дата обращения: 02.06.2020).

[226] Генсек ООН: пандемия коронавируса вызвала «цунами ненависти и ксенофобии» в мире [Электронный ресурс]. URL: https://www.vedomosti.ru/society/news/2020/05/08/829806-gensek-oon-prizval (дата обращения: 15.03.2020).

[227] Состояние преступности в России январь-декабрь 2019 г. [Электронный ресурс]. URL: http://crimestat.ru/ (дата обращения: 22.01.2021); Статистика террористической активности в России [Электронный ресурс]. URL: http://iminfin.ru/news/303-statistika-terroristicheskoj-aktivnosti-v-rossii (дата обращения: 04.12.2020).

ме того, по данным ФСБ РФ установлено 5,5 тыс. граждан России, входящих в ряд террористических организаций и воюющих в горячих точках, из них около 4 тыс. человек привлечено к уголовной ответственности.

В то же время снизилось количество зарегистрированных преступлений экстремистской направленности на 53,8 % и составило 585[228]. По данным Роскомнадзора, за последние 5 лет блокировано более 14 тысяч сайтов и удалено из российского сегмента сети Интернет в общей сложности более 140 тыс. материалов, призывающих к экстремизму и терроризму[229]. При этом следует отметить, что в настоящее время их становится меньше в сети Интернет, но в любых закрытых чатах мессенджеров они получили достаточное распространение.

Статистические показатели, касающиеся преступлений экстремистской направленности и их низкий уровень регистрации, свидетельствует, скорее о том, что в связи с развитием цифровых технологий меняются формы и способы совершения преступлений. Так, эти преступления, в большей своей части (80 % от общего числа выявленных преступлений экстремистской направленности) совершаются с использованием цифровых технологий[230].

Стремительное развитие информационно-коммуникационных и цифровых технологий позволяет террористам и экстремистам еще активнее расширять географию своей деструктивной идеологии, рекрутировать в свои ряды и привлекать финансовые средства, осуществлять хакерские атаки и другие преступления. Значительную поддержку деятельности экстремистских и террористических организаций оказывают социальные сети. Интернет стал для них, по сути, основным механизмом управления разрозненными силами и средствами, в том числе и финансовыми.

В настоящее время, по экспертным оценкам, насчитывается около 30 тысяч экстремистских и террористических сайтов, которые зачастую используются для вербовки своих сторонников, создание автономных ячеек, управление их деятельностью, сбора средств. Здесь же ведется подготовка к совершению экстремистских акций и террористических актов, а также освещению информации о проведенных мероприятиях.

---

[228] Состояние преступности в России январь–декабрь 2019 г. [Электронный ресурс]. URL: http://crimestat.ru/ (дата обращения: 18.08.2020).

[229] Роскомнадзор удалил более 140 тысяч материалов с призывами к экстремизму. [Электронный ресурс]. URL: https://ria.ru/20190801/1557081672.html?in=t (дата обращения: 29.12.2020).

[230] Около 80 % экстремистских преступлений в России совершается в интернете [Электронный ресурс]. URL: https://ria.ru/20190917/1558757896.html (дата обращения: 18.02.2021).

Все это позволяет сделать вывод о том, что наступила эра технологического и цифрового экстремизма и терроризма, а по масштабам последствий эта угроза в ближайшее время может быть сопоставима с оружием массового уничтожения. Так, например, за рубежом уже активно обсуждаются правыми радикалами конкретные цели и методы таких атак, в том числе «использование аэрозольных баллончиков, наполненных биологическими жидкостями от инфицированных людей, или распространение вируса при кашле или прикосновении к любой поверхности, используемой людьми в магазинах и в общественном транспорте»[231].

Переходя в эру цифровизации, экстремизм и терроризм становятся главной опасностью не только для России, но и других стран мира, поскольку использование сквозных цифровых технологий совместно с информационно-телекоммуникационными технологиями, повышает эффективность их преступной деятельности.

Особую тревогу вызывает появление новых форм названной преступной деятельности, что требует пересмотра и усовершенствования стратегии и тактики противодействия этим явлениям не только на уровне отдельно взятого государства, но и в целом во всем мировом сообществе. Особо следует обратить внимание на тот факт, что:

– все чаще стали использоваться: новые технологии при пропаганде экстремистской и террористической деятельности; новейшие разработки в области вооружения, цифровых технологий, иные способы, не требующие особой квалификации и длительной подготовки;

– изменилась тактика организации экстремистских и террористических объединений, ушли в прошлое длительные подготовки групп террористов (от 10 и более человек), если раньше стремились к созданию крупных организованных террористических объединений, то в настоящее время предпринимаются попытки организовать разветвленную сеть законспирированных террористических ячеек. Чаще стали использовать одиночек–террористов, что затрудняет их своевременное выявление, так как террорист–одиночка, как «иголка в стогу сена», его практически невозможно отследить. В то же время, как утверждает В. С. Овчинский, ссылаясь на Доклад Интерпола «среди террористов, совершивших реальные масштабные террористические акции, не было ни одного одиночки. Все подобные акции совершались сплоченными группами в составе 7 и более

[231] *Овчинский В. С.* Пандемия ненависти. Коронавирус несет не только болезнь, но и насилие в обществе [Электронный ресурс]. URL: http://zavtra.ru/blogs/pandemiya_nenavisti# (дата обращения: 26.06.2019).

человек. В то же время, согласно данным выборки, 29 % террористов были арестованы исключительно за одиночные действия. .... Либо они действительно осуществляли противозаконные действия в одиночку, либо, несмотря на все усилия правоохранительных органов, так и не сдали никого из своих подельников. Последующие исследования показали, что среди 30% указанных террористов были осведомлены о характере деятельности террористов. Более того, в 40 % случаях близкие друзья террористов сами не участвовали в подобного рода деятельности, но знали или догадывались о вовлеченности в терроризм своих друзей»[232]. Достаточно сложно определить и объект очередного террористического акта;

– увеличилось количество не только террористов одиночек, но и террористов смертников. Однако есть предположение того, что, например, «ИГИЛ перешло к бесструктурному управлению. Это означает, что террористы и им сочувствующие должны вести свою деятельность на основе самофинансирования не только изыскивая ресурсы, но и обеспечивая сами себя инструментами для проведения террористических актов. Эти акции, по мнению ИГИЛ, должны осуществляться не в результате сложных многофункциональных операций специально подготовленных групп, а в результате инициативы небольших команд – от 3–5 до максимум 10 человек[233] и направление будет меняться от крупных операций по проведению террористических актов к низкоуровневому доморощенному терроризму, то есть меняются объекты посягательств. Все чаще ими являются любые места массового скопления людей. Примером могут служить террористические акты, совершенные в 2017 г. в г. Санкт-Петербурге (3 апреля), в Египте (9 апреля), в Стокгольма (7 апреля), в Лондоне (22 марта), в Лас-Вегасе (2 октября);

– ведется активная работа по созданию разветвленной сети законспирированных террористических ячеек, вместо явно организованных террористических объединений;

– использование в совершении этих преступлений детей и женщин. Значительная часть преступлений крайне радикального характера в составе организованных преступных групп совершается несовершеннолетними. По некоторым данным «до 80 % участников группировок экстремистской и террористической направленности составляют молодые люди в возрасте

[232] *Овчинский В. С.* Иностранные боевики-террористы. Иногда они возвращаются. (Коллекция Изборского клуба). Москва: Книжный мир, 2019.

[233] *Там же.*

от 13 до 20 лет»[234]. Участились случаи радикализации несовершеннолетних через сайты и группы в соцсетях. В большинстве случаев под такое влияние попадают дети и подростки, которые попали в сложную жизненную ситуацию, лишены родительского внимания, имеют конфликты с одноклассниками и проблемы в общении со сверстниками. Как правило, радикальные идеи были им внедрены в сознание посредством тематических сайтов сети Интернет, которые активно формируют сетевые группы единомышленников, пропагандируя и распространяя деструктивную идеологию. При этом, мотивом для вступления в экстремистские группы подростков от 13 лет выступают «желание активной деятельности, стремление к индивидуальному самовыражению и общению с людьми, разделяющими их убеждения. Посеянная на такую благодатную почву агрессия проявляется в стремлении выразить протест и почувствовать свою независимость»[235]. Имеются данные об увеличении числа лиц в возрасте от 14 до 16 лет, прошедших обучение и боевую подготовку в МТО ИГ в сирийском городе Ракка[236];

– возросло количество террористов – приверженцев исламу, меняется стратегия и тактика их деятельности.

Но, самое главное, деятельность экстремистских и террористических организаций носит транснациональный характер. Она сегодня уже может «оказывать влияние на тенденции мирового развития, как политического, так и экономического характера и угрожающего поступательному развитию общества»[237].

Ни для кого не секрет, что активность экстремисткой и террористической деятельности определяется и находится в прямой зависимости от ее финансирования, поэтому проводится большая работа по перекрытию финансовых потоков. Так, например, Росфинмониторинг, совместно с правоохранительным органами, используя возможности межведомственной комиссии по противодействию финансированию терроризма блокировали банковские счета почти 5,5 тыс. лиц, подозреваемых в причастности к между-

---

[234] *Букреева О.* Защити своих детей от экстремизма и пропаганды терроризма! [Электронный ресурс]. URL: http://oxpaha.ru/national/zashhiti-svoih-detej-ot-ekstremizma-i-propagandy-terrorizma/ (дата обращения: 15.10.2017).

[235] *Там же.*

[236] URL: http://ru.valdaiclub.com/a/highlights/terrorizm-vo-frantsii-v-2015-godu/ (дата обращения: 15.12.2020); URL: http://ria.ru/society/20160419/1415127989.htm (дата обращения: 15.10.2017).

[237] *Горбунов Ю. С.* Глобализация терроризма // История государства и права. 2007. № 19.

народным террористическим организациям[238]. Вместе с тем финансирование экстремизма и терроризма получило не только широкий размах, но и новые формы и способы получения дополнительной финансовой помощи.

Известно, что основными источниками доходов экстремистских и террористических группировок, помимо сбора материальной помощи и взносов сторонников экстремизма и терроризма всегда являлись и являются незаконный оборот оружием, наркотиков, природных ресурсов и культурных ценностей, организация каналов нелегальной миграции, работорговля, сбыт фальшивых денег и пр. Они также активно участвуют в торгах на фондовых биржах через создаваемые подставные фирмы легально, вкладывают средства в недвижимость и различные отрасли экономики, получают средства от игры на фондовых рынках[239]. Особым способом финансирования сегодня для них является деятельность краудфандинга через онлайн-платформы, которые находятся в юрисдикции других государств, но которые позволяют собирать большое количество средств для экстремистских и террористических организаций.

При этом участились случаи использования в этих целях виртуальных активов (криптовалют), которая «не имеет централизованного эмитента, единого центра контроля за трансакциями и характеризуется анонимностью платежей»[240]. Все чаще используются так называемые конфиденциальные виртуальные активы, гарантирующие анонимность транзакций в отличие от биткоина и его аналогов.

Уровень криминологических угроз проявлений экстремизма и терроризма высок, как в целом по России, так и в отдельно взятых регионах. Так, Северо-Кавказский федеральный округ является одним из самых сложных регионов Российской Федерации. Террористическое подполье, несмотря на серьезные потери, сохраняет возможность для совершения террористических актов против мирных жителей. Что же касается региональных показателей, то больше всего этих преступлений было совершено в Дагестане

[238] Жертвами самых крупных терактов в 2019 году стали более 9 тысяч человек [Электронный ресурс]. URL: s://www.dp.ru/a/2019/10/13/ZHertvami_samih_krupnih_te (дата обращения: 27.08.2019).

[239] Жертвами самых крупных терактов в 2019 году стали более 9 тысяч человек [Электронный ресурс]. URL: s://www.dp.ru/a/2019/10/13/ZHertvami_samih_krupnih_te (дата обращения: 30.11.2020).

[240] Бастрыкин предложил приравнять фальсификацию истории к экстремизму [Электронный ресурс]. URL: https://rg.ru/2016/04/18/bastrykin-predlozhil-priravniat-k-ekstremizmu-falsifikaciiu-istorii.html (дата обращения: 15.10.2017).

(223 единицы), Чеченской Республике (89 единиц) и Кабардино-Балкарской Республике (82 единиц)[241]. Экстремистские, радикальные группировки пытаются активизировать свою деятельность не только на Северном Кавказе, но и перенести ее в другие регионы нашей страны. Именно они стремятся провоцировать межнациональные и межрелигиозные конфликты, ведут агрессивную пропаганду среди молодежи, используя самые современные информационные средства, технологии, включая интернет и социальные сети.

Все вышеизложенное свидетельствует о том, что криминологические угрозы распространения экстремизма и терроризма угрожают национальной безопасности России. Для снижения названных угроз потребуется постоянная работа по предотвращению этих явлений, при этом необходимо сотрудничество и с международными организациями, но в новом формате с использованием новых технологий и новых направлений противодействия этим явлениям.

[241] Статистика террористической активности в России [Электронный ресурс]. URL: http://iminfin.ru/news/303-statistika-terroristicheskoj-aktivnosti-v-rossii (дата обращения: 20.06.2018).

14.2. Проблемные вопросы предупреждения экстремизма и терроризма

Особое внимание конечно же уделяется предупредительной деятельности, направленной на устранение причин и условий, способствующих распространению экстремизма и терроризма в России. Государством принимаются «все меры для того, чтобы изменить ситуацию и снизить напряженность в этой сфере»[242]. На федеральном уровне принят ряд нормативных актов, определяющих основные принципы, задачи и цели противодействия экстремизму и терроризму, стратегию и тактику борьбы с названными явлениями[243].

Только в 2016 г. вступили в действие федеральные законы, усиливающие уголовную ответственность за преступления террористической и экстремистской направленности, расширен перечень преступлений, ответственность за которые наступает с 14-летнего возраста, уточнено понятие «финансирование терроризма». Уголовный кодекс Российской Федерации дополнен двумя статьями: ст. 205.6 (Несообщение о преступлении) и ст. 361 (Акт международного терроризма).

В России по инициативе ФСБ создан международный банк данных по противодействию терроризму, доступ к данным которого имеют уже 47 спецслужб из 36 стран, а также 8 специализированных органов международных организаций, включая ООН, СНГ, ШОС, ОДКБ и Интерпол. В настоящее время в нем размещены сведения о 116 террористических организациях и 43,5 тыс. лицах, причастных к терроризму, треть из них – это иностранные террористы-боевики[244].

---

[242] *Пинкевич Т. В.* Противодействие экстремизму: проблемы и особенности регионального уровня / Т. В. Пинкевич, О. А. Зубалова // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2012. № 17.

[243] Концепция общественной безопасности в Российской Федерации: Утверждена 14 ноября 2013 г. № Пр-2685. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 11.10.2017); Концепция противодействия терроризму в Российской Федерации: утв. Президентом Российской Федерации 5 октября 2009 г. Доступ из информационно-правового портала «Гарант» (дата обращения: 10.10.2017); О противодействии терроризму: федер. закон от 6 марта 2006 г. № 35-ФЗ. Доступ из информационно-правового портала «Гарант» (дата обращения: 17.10.2017); О Стратегии национальной безопасности Российской Федерации: указ Президента Российской Федерации от 31 декабря 2015 г. Доступ из информационно-правового портала «Гарант» (дата обращения: 15.10.2017); Об основах системы профилактики правонарушений в Российской Федерации: федер. закон от 23 июня 2016 г. № 182-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 01.10.2017).

[244] Обзор: ФСБ: В международный банк данных террористов внесены почти 44 тыс. человек [Электронный ресурс]. URL: https://eadaily.com/ru/news/2019/10/16/v-mezhdunarodnyy-bank-dannyh-terroristov-vneseny-pochti-44-tys-chelovek (дата обращения: 03.11.2019).

В связи с этим большое значение уделяется международному сотрудничеству. При этом, основными задачами в сотрудничестве противодействию терроризму в настоящее время, по мнению А. В. Бортникова, является «определение планов главарей террористических организаций, выявление основных маршрутов переброски иностранных террористов-боевиков и мест их концентрации, получение данных на каждого бандита, включая его интернет-профиль, при этом обмен информацией, по его словам, должен осуществляться в режиме реального времени»[245]. В связи с этим необходимы новые подходы к взаимодействию с целью повышения результативности и согласованности действий по предупреждению экстремизма и терроризма между странами, наращивая обмен значимой информацией и активизируя работу в информационной среде.

Но, как оказалось, этого недостаточно. Необходимо, прежде всего, принять меры общесоциального характера по минимизации причин и условий, способствующих проявлению экстремизма и терроризма, основными из которых являются: социально-политические, социально-экономические, культурно-воспитательные, организационно-правовые.

Специально-криминологические меры предполагают деятельность по устранению конкретных причин и условий, способствующих распространению экстремизма; выявлению и пресечению экстремистской деятельности общественных и религиозных объединений, иных организаций, физических лиц. Особое внимание должно уделяться созданию механизма предупреждения и нейтрализации социальных и межнациональных конфликтов и подготовке к совершенствованию мер профилактического, воспитательного и пропагандистского воздействия, направленных на предупреждение экстремистской деятельности.

Соответственно противодействие данным видам преступлений следует считать приоритетным в работе органов внутренних дел.

Особое место, конечно же, отводится средствам массовой информации и творческим организациям. Ведь ни для кого не секрет, что боевики используют Интернет и различные мессенджеры в первую очередь для пропаганды[246] и нельзя забывать, что социальные сети могут быть использованы для переубеждения таких лиц, противодействовать пропагандистской деятельности вербовщиков. Такая

[245] С начала 2019 года в России предотвратили 39 терактов [Электронный ресурс]. ТАСС. URL: https://tass.ru/politika/7006062 (дата обращения: 20.05.2020).

[246] Опасные клики. В совбезе прогнозируют серьезную активизацию террористов [Электронный ресурс]. URL: https://rg.ru/2020/10/20/v-sovbeze-rf-prognoziruiut-sereznuiu-aktivizaciiu-terroristov.html (дата обращения: 23.06.2021).

деятельность должна проводиться не только в сети Интернет, но и в прочих видах средств массовой информации.

Особую значимость имеет деятельность по осуществлению комплексных мероприятий по пропаганде российского законодательства. И в связи с этим в первую очередь необходимо:

– на всех уровнях организовать пропаганду российского законодательства, которая как общепрофилактическая мера воздействия на правонарушения по результатам социологического исследования используется только в 17 % случаях. А ведь такая пропаганда должна стать частью правового воспитания. Роль правового воспитания велика, она должна стать ведущей формой профилактической работы. При этом, необходима многоуровневая программа подготовки.

Федеральным законом «Об основах системы профилактики правонарушений в Российской Федерации» в качестве формы профилактического воздействия закреплено правовое просвещение и правовое информирование. В ст. 18 «Правовое просвещение и правовое информирование» указано, что в этих целях субъекты профилактики правонарушений или лица, участвующие в профилактике правонарушений, доводят до сведения граждан и организаций информацию, направленную на обеспечение защиты прав и свобод человека и гражданина, общества и государства от противоправных посягательств. При этом законодатель указывает, что такая информация «может доводиться до сведения граждан и организаций путем применения различных мер образовательного, воспитательного, информационного, организационного или методического характера»[247].

Особое внимание следует уделять разъяснению сущности правонарушений и преступлений, их общественной опасности, а также проведению активных мероприятий по формированию неприятия обществом, идеологии экстремистского и террористического характера, которое послужит снижению уровня радикализации различных групп населения, прежде всего молодежи, и недопущение их вовлечения в террористическую деятельность.

В сложившейся современной ситуации меры воспитательного характера граждан требуют особого внимания. При этом необходимо не только формирование нового типа молодежной культуры не насилия, а толерантности, диалога и взаимопонимания, способ-

[247] Об основах системы профилактики правонарушений в Российской Федерации: федер. закон от 23 июня 2016 г. № 182-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

ного активно противостоять проявлениям социального зла, внутренней и внешней агрессии.

Должна быть продолжена работа по пропаганде мирного сосуществования всех народов независимо от расы, национальности, языка, происхождения в противовес негативному информационно-идеологическому воздействию на личность извне, в том числе пропаганды идеологии терроризма.

– особый подход необходим к работе с лицами, возвратившимися к местам постоянного проживания, осужденных ранее за преступления террористического и экстремистского характера;

– внимания заслуживают и меры, направленные на предупреждение террористического наемничества среди молодежи. Тех, кто уже оказался под воздействием идеологии терроризма и экстремизма или может быть подвержен ей, необходима адресная профилактическая работа;

– на особый контроль должна быть поставлена работа по адаптации лиц, причастных к деятельности международных террористических организаций, в том числе и на территории Сирии и Ирака и вернувшихся в Россию. Данные меры в настоящее время необходимы, поскольку в 2016–2017 гг. в России выявлено более 3,5 тыс. граждан, подозреваемых в причастности к деятельности международных террористических организаций. К уголовной ответственности привлечено 1 719 российских граждан и граждан государств СНГ[248], из них 135 человек погибли в результате боестолкновений с правительственными войсками Сирии[249]. В 2019 г. ФСБ России установила 5,5 тыс. россиян, выехавших воевать в горячие точки в рядах террористических организаций, более 4 тыс. из которых были привлечены к уголовной ответственности. Кроме того, в Россию вернулись 337 боевиков, из них 224 осуждены и находятся в местах лишения свободы, 32 арестованы, в отношении остальных осуществляется сбор доказательной базы[250];

– деятельность по противодействию экстремизму и терроризму должна быть комплексной. Так, нельзя обходить стороной, напри-

---

[248] *Скворцов Ю. А.* Проблемы террористического наемничества среди молодежи и пути их преодоления//Международно-правовые средства противодействия терроризму в условиях глобализации. Проблемы террористического наемничества среди молодежи и пути их преодоления : сб. материалов Всероссийской научно-прак. конф. Ставрополь: СГПИ, 2016.

[249] Бастрыкин предложил приравнять фальсификацию истории к экстремизму. [Электронный ресурс]. URL: https://rg.ru/2016/04/18/bastrykin-predlozhil-priravniat-k-ekstremizmu-falsifikaciiu-istorii.html (дата обращения: 15.10.2019).

[250] С начала 2019 года в России предотвратили 39 терактов [Электронный ресурс]. URL: https://tass.ru/politika/70060622 (дата обращения: 16.10.2019).

мер, вопросы почти полной вооруженности населения отдельных субъектов Северо-Кавказского федерального округа, говоря о высоком уровне террористической угрозы. Если речь идет о распространении экстремизма и терроризма, то нельзя не учитывать вопросы миграции, наркотизации населения, влиянии миграционных процессов на рост теневой экономики, и пр.

Указав первоочередные меры, нельзя забывать о том, что противодействие терроризму и экстремистской деятельности являются основными направлениями профилактики правонарушений[251].

Такая деятельность должна осуществляться на основе государственной программы Российской Федерации в сфере профилактики правонарушений, а на ее основе приниматься целевые программы в сфере профилактики экстремизма и терроризма, включающие весь комплекс мер по устранению причин и условий, способствующих распространению этих явлений. В основу этих программ должны быть положены результаты: проведенного мониторинга состояния защищенности населения; определения степени его криминологической безопасности, выступающей составной частью общей системы национальной безопасности России; научных исследований в названной сфере. При этом, научно-обоснованная целевая программа, помимо указанного комплекса мер противодействия, в обязательном порядке должна включать полномочия субъектов обеспечения криминологической безопасности, основные направления, виды и формы их деятельности[252].

В связи с этим особое значение играет оснащенность подразделений по противодействию экстремизму и терроризму новейшими разработками, в том числе современными робототехническими комплексами, цифровыми технологиями для противодействия преступникам, поскольку «преступники располагают материалами, технологиями и инфраструктурой для производства химического оружия и биотоксинов, а для доставки поражающих элементов применяются беспилотные летательные аппараты»[253].

---

[251] Об основах системы профилактики правонарушений в Российской Федерации: федер. закон от 23 июня 2016 г. № 182-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

[252] *Пинкевич Т. В.* Экстремизм и терроризм: тенденции и проблемы противодействия в СКФО (региональный аспект) // Проблемы теории и практики борьбы с терроризмом и экстремизмом в России: материалы научно-практической конференции. Москва, Российская криминологическая ассоциация, Вестник Северо-Кавказского федерального университета. 2015.

[253] Бортников счел серьезной угрозой нарастания антиисламского терроризма [Электронный ресурс]. URL: https://www.interfax.ru/russia/661879 (дата обращения: 21.05.2019).

Такая деятельность должна осуществляться на основе государственной программы Российской Федерации в сфере профилактики правонарушений, а на ее основе приниматься целевые программы в сфере профилактики экстремизма и терроризма, включающие весь комплекс мер по устранению причин и условий, способствующих распространению этих явлений.

Контрольные вопросы

1. Раскройте особенности цифрового терроризма и экстремизма.
2. Определите причины распространения цифрового экстремизма и терроризма.
3. Назовите меры, принимаемые государством для снижения уровня угроз цифрового терроризма и экстремизма.
4. Дайте криминологическую характеристику цифровому терроризму и экстремизму.

Глава 15. Криминологическая характеристика преступности в сфере незаконного оборота наркотических средств и психотропных веществ в условиях цифровой трансформации

Планируемые результаты освоения темы главы

– **знать** особености преступности в сфере незаконного оборота наркотических средств и психотропных веществ в условиях развития цифровых технологий; основные показатели преступности;

– **уметь** определять особенности криминологической характеристики личности субъектов незаконного оборота наркотиков; использовать основные показатели преступности для оценки состояния названного вида преступности в стране;

– **владеть** юридической терминологией в сфере незаконного оборота наркотических средств и психотропных веществ в условиях развития цифровых технологий; навыками применения правил криминологического анализа.

15.1. Современное состояние преступности в сфере незаконного оборота наркотических средств и психотропных веществ и их прекурсоров

Результаты исследования незаконного оборота наркотических средств и психотропных веществ и их прекурсоров (далее наркотиков) в условиях развития цифровых технологий свидетельствует о том, что способы совершения названных преступлений, наркотизация населения, состояние законности, правопорядка и другие стороны жизни общества, приобрели новые современные формы, которые несомненно связаны с внедрением цифровых технологий. Нельзя забывать, что состояние наркотизма и наркомании в любом государстве или же в отдельно взятом регионе характеризуется рядом показателей: уровнем смертности от причин, связанных с употреблением наркотиков; количеством и уровнем зарегистрированных потребителей наркотиков и наркоманов; преступлений, связанных с незаконным оборотом наркотиков; структурой потребляемых наркотиков и т. п.[254]

[254] *Гилинский Я.* Девиантология. Санкт-Петербург.: Юридический центр Пресс, 2004.

Преступность в сфере незаконного оборота наркотиков это часть преступности, в то же время, являясь самостоятельным элементом ее структуры, представляет собой негативное социальное явление, включающее совокупность общественно опасных противоправных деяний, предусмотренных ст.ст. 228–233 УК РФ. Необходимость анализа преступности в сфере незаконного оборота наркотиков как самостоятельного структурного элемента общеуголовной преступности обусловлено не только ее количественной и структурной составляющей, сколько изменениями, происходящими в цифровом мире. Так, в России в последние годы наблюдается стойкая тенденция роста преступности исследуемого вида. При этом меняется этот вид преступности не только количественно, но и качественно, например, период с 1987 г. по 2015 г. количество зарегистрированных преступлений в сфере незаконного оборота наркотиков возросло более, чем в 16 раз[255].

Особо следует выделить период с 2016–2020 г.г., поскольку он отличается ростом не только количества совершенных преступлений в сфере незаконного оборота наркотиков, но и происшедшими коренными изменениями наркоситуации, которая складывается неоднозначно и обусловлена прежде всего ростом новых «дизайнерских наркотиков»[256], синтезированных наркотиков количество которых ежегодно возрастает (в среднем до 100 видов в год).

В первом полугодии 2020 г. впервые за много лет произошло снижение количества зарегистрированных преступлений, связанных с незаконным оборотом наркотиков (–0,5 % в сравнении с аналогичным периодом предыдущего года), удельный вес этих преступлений составил 9,4 %. При этом совершение названных преступлений в особо крупном размере возросло на 15,2 %. Возросло на 67,2 % числа выявленных фактов сбыта наркотиков, совершенных с использованием IT-технологий. При этом прослеживается уход действующих интернет-магазинов на платформе Hydra от продажи единичных закладок к более крупным партиям наркотиков весом от 5 до 100 грамм. Лиц, совершивших преступления в сфере незаконного оборота наркотиков, выявлено меньше на 7,7 %, чем за такой же период предыдущего года. Сопоставление данных показателей с показателями предыдущих лет дает основание полагать, что

---

[255] *Там же.*

[256] *Сибагатуллин А. М.* Уголовно-правовое и криминологическое противодействие незаконному обороту прекурсоров в России: дис. ... канд. юрид. наук. Краснодар, 2015.

правоохранительные органы стали меньше выявлять лиц, виновных в совершении названных преступлений.

Интересным представляется анализ преступности в сфере незаконного оборота наркотиков по видам. Чаще всего регистрируются деяния, предусмотренные ст.ст. 228 и 228.1 УК РФ, что составляет 96,4 % от общего числа преступлений, совершенных в сфере незаконного оборота наркотиков. При этом 62,3 % преступлений регистрируется по 228.1 УК РФ, только в первой половине 2020 г. количество совершенных преступлений, по сравнению с предыдущим годом, увеличилось на 3,4 %. В структуре нераскрытых наркопреступлений преобладают преступления, предусмотренные ст. 228.1 УК РФ (92,1 %). Криминальная активность населения по данному виду преступлений – 67,5 лиц на 100 тыс. населения.

Следует признать, что, несмотря на незначительные колебания, динамика преступности в сфере незаконного оборота наркотиков характеризуется тенденцией постоянного роста, увеличением количества преступлений, совершенных организованными группами, в крупном и особо крупном размере.

Кроме того, неумолимо растет рынок собственного нелегального производства высококонцентрированных синтетических наркотиков. Только за первое полугодие 2020 г. правоохранительными органами пресечена деятельность 242 нарколабораторий, что на 44 % больше, чем за такой же период предшествующего года. Особую популярность получил мефедрон. Сегодня на нелегальном рынке представлен их богатый ассортимент, поскольку химическая промышленность в стране развивается и без каких-либо затруднений можно приобрести не только приобрести прекурсоры, реактивы, но и необходимое химическое оборудование. Только за 4 месяца 2020 г. количество выявленных фактов незаконного оборота прекурсоров увеличилось на 86,4 %, при этом масса изъятых прекурсоров возросла в 24,3 раза.

И, еще одна примета современной наркоситуации заключается в том, что названная преступная деятельность находится под жестким контролем организованной преступности, но за редким исключением привлекаются к уголовной ответственности руководители преступного сообщества или организованной группы, поскольку их деятельность, как правило, непосредственно связана с цифровыми технологиями и такими цифровыми платформами, как Tor, Hydra, DarkNet и др.

Они используют более безопасную блочно-сетевую структуру, что позволяет взаимодействовать, общаться только дистанционно по сети Интернет или мобильной связи, через всевозможные мессен-

джеры Viber, WhatsApp и Telegram и социальные сети «Одноклассники», «ВКонтакте», Facebook и Twitter. Наличие телефонов с установленными программами персональной связи и приложениями для защищенных переговоров, обменов сообщениями, фотографиями и видео конфиденциального характера, содержащими защищенные от взлома хранилища видео-, фотофайлов, позволяет «работать» в любом регионе и быстро принимать решение по смене дислокации, с одной стороны. А с другой, такие приложения позволяют их администраторам централизованно координировать все совершаемые соучастниками действия, направленные на незаконный оборот наркотиков, которые входят в состав различных преступных групп. Их деление осуществляется в зависимости от количества интернет-магазинов, объема поступающего «товара» и т. п., но решение принимает, естественно, руководитель. Каждому из созданных интернет-магазинов для связи с потенциальными покупателями приобретаются абонентские телефонные номера различных операторов связи, зарегистрированные на подставных лиц, и проводится их регистрация в программах обмена почтовыми сообщениями[257].

Этот криминальный вид деятельности является не только высокоприбыльным, но и высоко латентным, поскольку их преступная деятельность осуществляется бесконтактно. По данным TOR Metrics, Россия сегодня занимает второе место в мире после США по числу пользователей «теневого» Интернета в секторе продажи наркотиков. Ежедневно в анонимную сеть выходят около 300 тыс. россиян, что составляет 11 % общемирового числа пользователей DarkNeta[258].

Особой популярностью пользуются различные системы анонимайзеров. Для перевода денежных средств применяются электронные платежи WebMoney, QIWI и «Яндекс. Деньги». Товар продавался на условиях 100 % предоплаты, которая осуществлялась через Webmoney, «Яндекс.Деньги», «Qiwi-кошелек».

По данным 2019 г., только на русскоговорящем ресурсе «Гидра» (Hydra) занимаются продажей каннабиса около 1,5 тыс. сервисов, стимуляторов – 1,3 тыс., экстази – 500, каннабиоидов – 200 сервисов и т. д. Новым трендом является растущее предложение так называемых химических конструкторов, позволяющих пользователю самостоятельно изготовлять наркотики. При этом оплата этих

[257] *Ализаде В. А.* Судебная практика по делам о преступлениях в сфере незаконного оборота наркотиков, совершенных с использованием криптовалюты: от разных подходов к предложению единого понимания / В. А. Ализаде, А. Г. Волеводз // Библиотека криминалиста. 2018. № 1 (36).

[258] URL: https://metrics.torproject.org/bandwidth.html (дата обращения: 08.12.2019).

конструкторов в 100 % случаев осуществляется с использованием криптовалюты[259].

Как показывает практика, осуществив анонимную предварительную оплату сбытчику наркотиков, наркотики передаются бесконтактным способом. Как правило, это закладки и тайники, место нахождение которых уточняется и передается покупателю с использованием цифровых технологий. Известно, что в социальных сетях, в группах по интересам, на форумах развлекательных порталов идет обсуждение о видах наркотиках, их поставках, приобретении и использовании. Более того, для рекламы о сбыте наркотиков создаются специальные сайты. Сегодня не является секретом тот факт, что незаконный оборот наркотиков способствует увеличению объемов теневого оборота капитала, в том числе и легализации (отмыванию) преступных доходов.

Результаты исследования позволили определить ролевой состав преступных сообществ и организованных групп, включающий организатора, менеджера по персоналу, финансиста-бухгалтера, администраторов (диспетчеров) территорий, руководителя. Как правило, они относятся к категории «неустановленное лицо» и за редким исключением могут быть привлечены к уголовной ответственности. Администраторы (диспетчеры) территорий взаимодействуют с руководителями организованных преступных групп. При этом руководитель может взаимодействовать в онлайн режиме с несколькими организованными группами, которые между собой не связаны преступной деятельностью, а каждая действует автономно. В его задачи входит общее руководство деятельностью группы; координация деятельности ее членов, путем дачи указаний использования сети «Интернет» и программы интерактивного общения «Телеграм»; координация действий администратора (диспетчера) разработка плана совершаемых преступлений, полностью исключающего как саму возможность визуального контакта сбытчика и покупателя наркотических средств, так и визуальный контакт между самими участниками группы. Договоренность о приобретении наркотического средства между соучастниками и покупателем осуществляется только путем общения в ходе переписки посредством мобильной связи, с использованием сети Интернет или программы «Телеграм». В такую организованную группу входят поми-

[259] *Иванцов С. В.* Преступления, связанные с использованием криптовалюты: основные криминологические тенденции / С. В. Иванцов, Э. Л. Сидоренко, Б. А. Спасенников, Ю. М. Берёзкин, Я. А. Суходолов // Всероссийский криминологический журнал. 2019. Т. 13. № 1.

мо организатора кураторы интернет-магазинов, складов, операторы, курьеры и закладчики. Последние из пяти названных, как правило, и привлекаются к уголовной ответственности по ст. 2281 УК РФ.

Численность таких групп может достигать 5 до 50 человек и более, а высокая степень организации преступной деятельности и принятые меры конспирации позволяют таким группам в течение длительного периода оставаться не разоблаченными правоохранительными органами и совершать ряд тяжких и особо тяжких преступлений в сфере незаконного оборота наркотических средств и психотропных веществ.

Почти в каждом уголовном деле, в описательной части указываются способы оплаты и получения вознаграждения за преступную деятельность, связанную с незаконным оборотом наркотиков. Так, например, руководитель организованной преступной группы разрабатывает схему легализации доходов, полученных преступным путем, в целях конспирации преступной деятельности, сокрытия источников происхождения полученных доходов и придания правомерного вида владению, пользованию и распоряжению денежными средствами, полученными от совершения тяжких и особо тяжких преступлений в сфере незаконного оборота наркотиков и использует в своей преступной деятельности виртуальный счет криптовалютного кошелька а затем реализуя свой умысел на легализацию (отмывание) доходов, полученных преступным путем, криптовалюта конвертируется в безналичные российские рубли, которые обналичивают их в банкоматах. Таким образом, он своими действиями с денежными средствами, приобретенными в результате совершения преступления, в целях придания правомерного вида владению пользованию и распоряжению указанными денежными средствами, совершил преступление, предусмотренное ст. 1741 УК РФ.

При этом используют блочно-сетевую структуру, что позволяет не взаимодействовать, общение только дистанционное по сети Интернет или мобильной связи, через всевозможные мессенджеры, которые мы уже называли.

В целом, в современной России негативные тенденции в сфере незаконного оборота наркотиков продолжают нарастать. Несмотря на огромную работу, которая проводится в рамках реализации государственной антинаркотической политики, требуется повысить эффективность не только правоприменительной деятельности, но и обратиться к вопросам законодательного регулирования оборота наркотических средств и психотропных веществ.

15.2. Причинный комплекс и вопросы противодействия незаконному обороту наркотических средств и психотропных веществ

Предупреждение преступности может быть эффективным только в случае, если оно базируется на адекватном представлении государства о специфике ее криминогенных детерминант, состоящих из комплекса причин и условий преступности, темпы роста которой превратились в одну из главных угроз национальной безопасности страны.

Известно, что Россия, в последние годы, стала объектом экспансии международного наркобизнеса. Причиной этому является тот факт, что в трех северных провинциях Афганистана – Бадахшане, Кундузе, Тахаре – сконцентрированы основные мощности по производству героина и выращиванию опиумного мака, поступающего в страны Организации Договора о коллективной безопасности, при чем он отличается высокой токсичностью. Неслучайно в рамках Соглашения о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступностью (г. Москва, 25 ноября 1998 года), Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с незаконным оборотом наркотических средств, психотропных веществ и прекурсоров (г. Минск, 30 ноября 2000 года) проводится серьезная работа в данном направлении. Так, только в первой половине 2019 года в Российской Федерации из незаконного оборота изъято 7,6 т наркотических средств, в том числе 333,5 кг наркотиков опийной группы.

Социально-экономические составляющие причинного комплекса исследуемых социальных явлений напрямую связаны с занятостью населения, во-первых, лица, имеющие постоянный источник дохода и возможность тем самым обеспечить себя и своих близких, в структуре осужденных за эти преступления занимают незначительный процент (2–3 %). Во-вторых, сказывается неблагоприятная социально-экономическая обстановка (миграционный отток населения, спад уровня производства, безработица, рост уровня теневой экономики).

Следующей причиной, способствующей незаконному обороту наркотиков, является коррупция, позволяющая лицам, совершающим данные преступления, не быть уверенными в неотвратимости соответствующего наказания за это. Наркобизнес не мог бы существовать и, тем более, развиваться, если бы не тесная, тай-

ная, а порой и открытая, связь преступности с государственными служащими. Однако наркобизнес как один из видов организованной преступности использует для достижения своих целей не только коррупцию, но и такие методы воздействия на чиновников, как шантаж или насилие.

Значительную роль в причинном комплексе преступности играют факторы духовно-нравственного характера, это касается и преступности исследуемого вида. Высокий уровень правового и нравственного нигилизма, как правило, выражается в игнорировании требований и предписаний законов и норм морали.

Не в меньшей мере на рост преступности данного вида влияют и социально-психологические обстоятельства, прежде всего, молодого поколения страны. Утрата идейно-нравственных ориентиров, сформированных в прежние годы, породила у части молодежи пассивность, нравственную деградацию, скептицизм, стремление забыться от всего, и «расслабиться». Организационно-управленческие факторы связаны с отсутствием длительное время в нашей стране комплексных мер противодействия незаконному обороту наркотиков.

Известно, что социально-экономические и политические изменения, произошедшие в стране, отразились и на свойствах личности преступника как одного из главных элементов незаконного оборота наркотиков. В то же время с развитием информационно-телекоммуникационных технологий, а затем цифровых технологий произошли существенные изменения в социуме, в том числе и виртуальном, которые изменили и личность преступника.

Говоря о структуре личности преступника, следует отметить, что она включает в себя совокупность свойств, которые образуются в процессе многообразного и систематического взаимодействия с другими людьми, и делающих в свою очередь ее субъектом деятельности, познания и общения. Именно поэтому для изучения личности преступника, его криминологической характеристики в криминологической доктрине исследуют три группы признаков: социальный статус личности, социальные функции (роли) личности[260], нравственно-психологические качества, ценностные ориентации[261].

Характер преступного поведения человека во многом зависит от его возраста. Данный вид преступности с каждым годом молоде-

---

[260] Криминология: учебник // под ред. Н. Ф. Кузнецовой, Г. М. Миньковского. Москва, 1998; Криминология: учебник для вузов // под ред В. Д. Малкова. Москва, 2008.

[261] Криминология: учебник // под ред. В. Н. Бурлакова, В. П. Сальникова. Санкт-Петербург, 1998; Криминология: учебник для вузов // под ред В. Д. Малкова. Москва, 2008.

ет, как правило эти преступления совершаются лицами в возрасте 18–29 лет. Большая часть преступлений совершается лицами мужского пола, но следует признать, что их количество незначительно превышает количество женщин, совершивших такие же преступления (мужчины – 54,1%, женщины – 45,1 %). При этом большая часть женщин, совершивших эти преступления, не имеет постоянного места жительства, а большая часть осужденных за данные преступления не имеет высшего образования. Увеличилось количество лиц, совершивших преступления, не имеющих постоянных источников доходов, в том числе безработных, о 43,8 % лиц до совершения преступления не могли устроиться на работу из-за общей безработицы.

Анализируя личность преступника, необходимо обратить внимание и на его нравственно-психологические признаки. К ним, в первую очередь, следует отнести внутреннюю позицию личности в различных сферах социального бытия, поскольку именно она способствует деформации нравственно-психологических качеств. Нельзя в связи с этим не учитывать морально-волевые позиции личности, ее потребности и интересы. Совокупность всех этих показателей дает возможность определить ее качественную характеристику и позволяет определять личную установку преступника. Именно они помимо содеянного им определяют общественную опасность личности преступника.

Безусловно, исследование причинного комплекса и личности преступника, а также сам факт, что незаконный оборот наркотиков является «доминирующим свойством в детерминационном механизме»[262].

Особое место в причинном комплексе занимает вопрос транснационального ее характера и рост количества преступлений, совершаемых с использование информационных и телекоммуникационных сетей, в том числе и сети Интернет. Это обусловливает необходимость подготовки соответствующих криминологических мер противодействия современному незаконному обороту наркотиков, который осуществляется с использованием цифровых технологий. В данном случае необходимо продолжать совместные с международным сообществом мероприятия по противодействию распространения незаконного оборота наркотиков.

---

[262] *Сибагатуллин А. М.* Уголовно-правовое и криминологическое противодействие незаконному обороту прекурсоров в России: дис. ... канд. юрид. наук А. М. Сибагатуллина. Краснодар, 2015.

На этом уровне необходимо в целях сотрудничества проводить рабочие встречи по вопросам обмена положительным опытом работы и координации совместных действий по борьбе с незаконным оборотом наркотиков; осуществлять взаимодействие по перекрытию каналов поступления наркотиков и расширить практику проведения согласованных операций и оперативно-розыскных мероприятий, связанных с незаконным оборотом.

Активизировать взаимообмен информацией: о лидерах и активных участниках международных преступных сообществ (преступных организаций), причастных к незаконному наркотических средств, психотропных веществ и прекурсоров; о новых методах распространения и сбыта наркотических средств, психотропных веществ и прекурсоров; об использовании в преступных целях современных информационно-телекоммуникационных технологий; о принадлежности IP-адресов, абонентских номеров телефонов, аккаунтов, кошельков электронных платежных систем и криптовалют, электронных идентификаторов в случае взаимной заинтересованности в разработке лиц, участвующих в распространении наркотиков. Установление международных и межрегиональных преступных связей лиц, причастных к незаконному обороту наркотиков и постоянное проведение мониторинга по изучению всего причинного комплекса преступности. Это направление деятельности необходимо для того чтобы стремиться к устранению причинного комплекса распространения незаконного оборота наркотиков и пресечения и предотвращения этих преступлений.

Необходимо осуществлять системный подход к информационному обмена данными между правоохранительными органами Российской Федерации:

а) о лидерах и активных участниках организованных преступных групп и преступных сообществ;

б) о фактах незаконного оборота незаконного оборота наркотических средств, психотропных веществ и прекурсоров с использованием цифровых технологий;

в) о преступных связях участников транснациональных преступных групп, а также розыска лиц, совершивших преступления в сфере незаконного оборота наркотических средств, психотропных веществ и прекурсоров;

г) о пресечении каналов распространения наркотических средств, психотропных веществ и прекурсоров с использованием цифровых технологий и дистанционной торговли;

д) о сборе своевременной информации о раскрытии и расследовании преступлений, связанных с незаконным оборотом наркотических средств, психотропных веществ и прекурсоров, связанных с из в значительном размере, а также синтетических наркотиков и курительных смесей;

е) об изменениях наркоситуации, о путях и маршрутах транспортировки наркотических средств, психотропных веществ и прекурсоров;

ж) о выявлении и пресечении новых способов поставок и маршрутов поставки наркотических средств, психотропных веществ и прекурсоров.

Учитывая, что при незаконном обороте наркотических средств, психотропных веществ и прекурсоров широкое распространение получило использование цифровых технологий, необходимо в области противодействия незаконному обороту наркотиков:

– осуществлять на постоянной основе профессиональную подготовку и переподготовку сотрудников антинаркотических подразделений МВД России с изучением работы и функционала цифровых технологий с целью повышения эффективности деятельности по раскрытию и расследованию этих преступлений, совершаемых с использованием цифровых технологий, обучать сотрудников правоохранительных органов приемам и способам обнаружения сокрытий и ухищрений, выявления незаконных операций с наркотиками;

– создавать правовые и организационно-технические (кадровое, материально-техническое обеспечение) условия для эффективной деятельности правоохранительных органов по противодействию их незаконному обороту;

– активизировать работу по противодействию легализации (отмыванию) денежных средств или иного имущества, полученных в результате совершения этих преступлений;

– осуществлять постоянный мониторинг потоков денежных средств с целью установления незаконных финансовых операций и выявления предикатных преступлений, совершенных в сфере незаконного оборота наркотиков;

– во взаимодействии с Федеральной службой по финансовому мониторингу и правоохранительными органами проводить мероприятия по установлению лиц, причастных к финансовым операциям, связанным с названными средствами и веществами;

– осуществлять повышение эффективности координации и взаимодействия между правоохранительными органами и их подразделениями.

Данная деятельность может быть успешной только в том случае, когда она будет осуществляться на основе целевых программ, включающих весь комплекс мер по устранению причин и условий, способствующих незаконному обороту наркотических средств, психотропных веществ и прекурсоров, совершаемых с использованием цифровых технологий.

Контрольные вопросы

1. Проанализируйте современное состояние преступности в сфере незаконного оборота незаконного оборота наркотических средств, психотропных веществ и прекурсоров.

2. Какова специфика незаконного оборота наркотических средств, психотропных веществ и прекурсоров, совершаемого с использованием цифровых технологий?

3. Определите уровень латентности незаконного оборота наркотических средств, психотропных веществ и прекурсоров, совершаемого с использованием цифровых технологий.

4. Проанализируйте меры предупреждения незаконного оборота наркотических средств, психотропных веществ и прекурсоров, совершаемого с использованием цифровых технологий.

СПИСОК РЕКОМЕНДОВАННЫХ НОРМАТИВНО-ПРАВОВЫХ АКТОВ И ЛИТЕРАТУРЫ

Перечень основных нормативно-правовых актов, регулирующих вопросы цифровой экономики

I) Нормативно-правовые акты Российской Федерации:

1. Конституция Российской Федерации (принята всенародным голосованием 12 декабря 1993 г. с изменениями, одобренными в ходе общероссийского голосования 01.07.2020). Доступ из справ.-правовой системы «КонсультантПлюс».

2. Уголовный кодекс Российской Федерации от 13 июня 1996 г № 63-ФЗ (с послед. измен. и доп.) // Собр. законодательства Рос. Федерации. 1996. № 25. Ст. 2954.

3. О безопасности критической информационной инфраструктуры Российской Федерации: федер. закон от 26 июля 2017 г. № 187-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

4. О безопасности: федер. закон от 28 декабря 2010 г. № 390. Доступ из справ.-правовой системы «Консультант плюс».

5. О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации: федер. закон от 18 март 2019 г. № 34-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

6. О государственной тайне: закон Российской Федерации от 21 июля 1993 г. № 5485-1-ФЗ (ред. от 29.07.2018). Доступ из справ.-правовой системы «КонсультантПлюс».

7. О защите детей от информации, причиняющей вред их здоровью и развитию: федер. закон Российской Федерации от 29 декабря 2010 г. № 436-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

8. О коммерческой тайне: федер. закон от 29 июля 2004 г. № 98-ФЗ (ред. от 18.04.2018). Доступ из справ.-правовой системы «КонсультантПлюс».

9. О наркотических средствах и психотропных веществах: федер. закон от 8 января 1998 г. № 3-ФЗ // Собр. законодательства Рос. Федерации. 2012. № 10. Ст. 1166.

10. О персональных данных: федер. закон от 27 июля 2006 г. № 152-ФЗ (ред. от 31.12.2017). Доступ из справ.-правовой системы «КонсультантПлюс».

11. О полиции: федер. закон от 7 февраля 2011 г. № 3-ФЗ // Собр. законодательства Рос. Федерации. 2011. № 7. Ст. 900.

12. О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации: федер. закон от 2 августа 2019 г. № 259-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

13. О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма: федер. закон от 7 августа 2001 г. № 115-ФЗ (ред. от 18.03.2019) (с изм. и доп., вступ. в силу с 27.06.2019). Доступ из справ.-правовой системы «КонсультантПлюс».

14. О связи: федер. закон от 7 июля 2003 г. № 126-ФЗ (ред. от 06.06.2019, с изм. и доп., вступ. в силу с 01.11.2019). Доступ из справ.-правовой системы «КонсультантПлюс».

15. Об информации, информационных технологиях и о защите информации: федер. закон от 27 июля 2006 г. № 149-ФЗ (ред. от 19.07.2018). Доступ из справ.-правовой системы «Консультант Плюс».

16. Об основах системы профилактики правонарушений в Российской Федерации: федер. закон от 23 июня 2016 г. № 182-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

17. Доктрина информационной безопасности Российской Федерации: указ Президента Российской Федерации от 5 декабря 2016 г. № 643. Доступ из справ.-правовой системы «КонсультантПлюс».

18. О мерах по противодействию терроризму: указ Президента Российской Федерации от 15 февраля 2006 г. № 116 (ред. от 25 ноября 2019). Доступ из справ.-правовой системы «КонсультантПлюс».

19. О мерах по совершенствованию государственного управления в области противодействия терроризму: указ Президента Российской Федерации от 26 декабря 2015 г. № 664 (ред. от 21.02.2019). Доступ из справ.-правовой системы «КонсультантПлюс».

20. О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года: указ Президента Российской Федерации от 7 мая 2018 г. № 204 (ред. от 19.07.2018). Доступ из справ.-правовой системы «КонсультантПлюс».

21. О развитии искусственного интеллекта в Российской Федерации (вместе с Национальной стратегией развития искусственного интеллекта на период до 2030 года): указ Президента Российской

Федерации от 10 октября 2019 г. № 490. Доступ из справ.-правовой системы «КонсультантПлюс».

22. О совершенствовании государственного управления в сфере контроля за оборотом наркотических средств, психотропных веществ и их прекурсоров и в сфере миграции: указ Президента Российской Федерации от 5 апреля 2016 г. № 156 // Собр. законодательства Рос. Федерации. 2016. № 15. Ст. 2071.

23. О Стратегии научно-технологического развития Российской Федерации: указ Президента Российской Федерации от 1 декабря 2016 г. № 642. Доступ из справ.-правовой системы «КонсультантПлюс».

24. О Стратегии национальной безопасности Российской Федерации: указ Президента Российской Федерации от 31 декабря 2015 г. № 683. Доступ из справ.-правовой системы «КонсультантПлюс».

25. О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: указ Президента Российской Федерации от 9 мая 2017 г. № 203. Доступ из справ.-правовой системы «КонсультантПлюс».

26. Об утверждении Доктрины информационной безопасности Российской Федерации: указ Президента Российской Федерации от 5 декабря 2016 г. № 646. Доступ из справ.-правовой системы «КонсультантПлюс».

27. Об утверждении Правил определения перечня организаций и физических лиц, в отношении которых имеются сведения об их причастности к экстремистской деятельности или терроризму, и доведения этого перечня до сведения организаций, осуществляющих операции с денежными средствами или иным имуществом, и индивидуальных предпринимателей: постановление Правительства Российской Федерации от 6 августа 2015 г. № 804 (ред. от 11.09.2018). Доступ из справ.-правовой системы «КонсультантПлюс».

28. О Концепции долгосрочного социально-экономического развития Российской Федерации на период до 2020 года (вместе с Концепцией долгосрочного социально-экономического развития Российской Федерации на период до 2020 года): распоряжение Правительства Российской Федерации от 17 ноября 2008 г. № 1662-р (ред. от 28.09.2018). Доступ из справ.-правовой системы «КонсультантПлюс».

29. О плане мероприятий («дорожной карте») по совершенствованию законодательства и устранению административных барьеров в целях обеспечения реализации Национальной технологической

инициативы по направлению «Технет» (передовые производственные технологии): распоряжение Правительства Российской Федерации от 23 марта 2018 г. № 482-р. Доступ из справ.-правовой системы «КонсультантПлюс»;

30. Об утверждении программы «Цифровая экономика Российской Федерации»: распоряжение Правительства Российской Федерации от 28 июля 2017 г. № 1632-р. Доступ из справ.-правовой системы «КонсультантПлюс».

31. Об утверждении Стратегии развития отрасли информационных технологий в Российской Федерации на 2014–2020 годы и на перспективу до 2025 года: распоряжение Правительства Российской Федерации от 1 ноября 2013 г. № 2036-р (ред. от 18.10.2018). Доступ из справ.-правовой системы «КонсультантПлюс».

32. Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (утв. Президентом Российской Федерации 12 декабря 2014 г. № К-1274. Доступ из справ.-правовой системы «КонсультантПлюс».

33. Концепция общественной безопасности в Российской Федерации (утв. Президентом Российской Федерации 20 ноября 2013 г.). Доступ из справ.-правовой системы «КонсультантПлюс».

34. Концепция противодействия терроризму в Российской Федерации (утв. Президентом Российской Федерации 5 октября 2009 г.). Доступ из справ.-правовой системы «КонсультантПлюс».

35. Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы (утв. указом Президента Российской Федерации от 9 мая 2017 г. № 203). Доступ из справ.-правовой системы «КонсультантПлюс».

36. Стратегия противодействия экстремизму в Российской Федерации до 2025 года (утв. указом Президента Российской Федерации 29 мая 2020 г. № 344). Доступ из справ.-правовой системы «КонсультантПлюс».

37. О внесении изменений в Гражданский кодекс Российской Федерации в части совершенствования правового регулирования отношений в области робототехники [Электронный ресурс]: проект федер. закона от 2017 г. URL: http://robopravo.ru/proiekty_aktov (дата обращения: 20.05.2020).

38. О внесении изменений в части первую, вторую и четвертую Гражданского кодекса Российской Федерации: проект федер. закона № 424632-7 (ред., внесенная в Государственную Думу Федерального Собрания Российской Федерации, текст по состоянию

на 26.03.2018). URL: https://sozd.duma.gov.ru/bill/424632-7 (дата обращения: 03.12.2019).

39. Об утверждении Концепции построения и развития узкополосных беспроводных сетей связи «Интернета вещей» на территории Российской Федерации [Электронный ресурс]: приказ Минкомсвязи России от 29 марта 2019 г. URL: http://docs.cntd.ru/document/554066760 (дата обращения: 01.07.2019).

40. Модельная конвенция о робототехнике и искусственном интеллекте 2017 года [Электронный ресурс]. URL: http://www.iksmedia.ru/news/5453922-V-Rossii-razrabotan-proekt-pervoj.html.

II) Международно-правовые документы:

1. О ратификации соглашения о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации: федер. закон от 1 октября 2008 г. № 164-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

2. Об участии Российской Федерации в деятельности Международной организации уголовной полиции – Интерпола: указ Президента Российской Федерации от 30 июля 1996 г. № 1113 (ред. от 27.10.2011) // Собр. Законодательства Рос. Федерации. № 32. Ст. 3895.

3. О признании утратившим силу распоряжения Президента Российской Федерации от 15 ноября 2005 г. № 557-рп «О подписании Конвенции о киберпреступности»: распоряжение Президента РФ от 22 марта 2008 г. № 144-рп. Доступ из справ.-правовой системы «КонсультантПлюс».

4. ISO 13482: 2014 Роботы и роботизированные устройства. Требования безопасности для роботов личной гигиены (ISO 13482:2014 Robots and robotic devices – Safety requirements for personal care robots) [Электронный ресурс]. URL: https://www.iso.org/obp/ui/ru/#iso:std:iso:13482:ed-1:v1:en .

5. Aconf.187/10 Справочный документ для семинара-практикума по преступлениям, связанным с использованием компьютерной сети [Электронный ресурс]. URL: file:///C:/Users/Ekaterina/Downloads/A_CONF.187_10-RU.pdf.

6. Арабская конвенция о борьбе с преступлениями в области информационных технологий (Каир, 21.12.2010) [Электронный ресурс]. URL: www.https://www.ebrary.net/57669/law/league_arab_states.

7. Декларация о сотрудничестве в рамках европейского партнерства в сфере блокчейн-технологий (принята в г. Брюсселе

10.04.2018) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

8. Декларация принципов «построение информационного общества – глобальная задача в новом тысячелетии» (Женева, 2003) [Электронный ресурс]. URL: https://online.zakon.kz/Document/?doc_id=30170561#pos=7;129.

9. Декларация принципов и программа действий программы Организации Объединенных Наций в области предупреждения преступности и уголовного правосудия (приняты резолюцией 46/152 Генеральной Ассамблеи от 18 декабря 1991 года) [Электронный ресурс]. URL: http://www.un.org/ru/documents/.

10. Конвенция о защите прав человека и основных свобод от 4 ноября 1950 г. Доступ из справ.-правовой системы «КонсультантПлюс».

11. Конвенция о защите физических лиц при автоматизированной обработке персональных данных (заключена в г. Страсбурге 28.01.1981) (вместе с Поправками к Конвенции о защите физических лиц при автоматизированной обработке персональных данных (СДСЕ № 108), позволяющими присоединение европейских сообществ, принятыми Комитетом Министров в Страсбурге 15.06.1999). Доступ из справ.-правовой системы «КонсультантПлюс».

12. Конвенция о кибербезопасности и защите персональных данных (Ball K. M. African Union Convention on Cyber Security and Personal Data Protection). International Legal Materials. 2017. Vol. 56. Iss. 1.

13. Конвенция о преступности в сфере компьютерной информации (ETS N 185) (заключена в г. Будапеште 23.11.2001) (с изм. от 28.01.2003). Доступ из справ.-правовой системы «КонсультантПлюс».

14. Конвенция Организации Объединенных Наций о борьбе против незаконного оборота наркотических средств и психотропных веществ (заключена в г. Вене 20.12.1988). Доступ из справ.-правовой системы «КонсультантПлюс».

15. Модельный Регламент административных процедур, осуществляемых уполномоченными органами в сфере обеспечения информационной безопасности государств – участников СНГ от 28 ноября 2014 г. Доступ из справ.-правовой системы «КонсультантПлюс».

16. Модельный закон СНГ о критически важных объектах информационно-коммуникационной инфраструктуры от 28 ноября 2014 г. Доступ из справ.-правовой системы «КонсультантПлюс».

17. Директивы ОЭСР по проблеме безопасности информационных систем и сетей: формирование культуры обеспечения без-

опасности [Электронный ресурс]. URL: https://www.oecd.org/sti/ieconomy/15582276.pdf.

18. Регламент Европейского Парламента и Совета Европейского Союза 2016/679 от 27 апреля 2016 г. о защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/EC (Общий Регламент о защите персональных данных / General Data Protection Regulation /GDPR). Доступ из информационно-правового портала «Гарант».

19. Резолюция 415 (V) Генеральной Ассамблеи ООН «Передача функций международной уголовной и пенитенциарной комиссии» от 1 декабря 1950 г. [Электронный ресурс]. URL: http://www.un.org/ru/ga/5/docs/5res.shtml.

20. Резолюция A/RES/53/70 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» от 4 января 1999 г. [Электронный ресурс]. URL: https://www.ifap.ru/ofdocs/un/5753.pdf.

21. Резолюция Европарламента от 16 февраля 2017 г. 2015/2013(INL) P8_TA-PROV (2017)0051, включает текст Хартии робототехники [Электронный ресурс]. URL: http://robopravo.ru/riezoliutsiia_ies.

22. Рекомендации Межпарламентской ассамблеи государств СНГ по совершенствованию законодательства государств – участников СНГ в сфере противодействия технологичному терроризму от 16 апреля 2015 г. Доступ из справ.-правовой системы «КонсультантПлюс».

23. Рекомендации относительно международного сотрудничества в области предупреждения преступности и уголовного правосудия в контексте развития (приняты 14 декабря 1990 г. Резолюцией 45/107 на 68-ом пленарном заседании Генеральной Ассамблеи ООН). Доступ из справ.-правовой системы «КонсультантПлюс».

24. О сотрудничестве в области предупреждения преступлений: рекомендация № Rec (2003) 21 Комитета министров Совета Европы (принята 24 сентября 2003 г. на 853-м заседании представителей министров). Доступ из справ.-правовой системы «Консультант Плюс».

25. О Концепции взаимодействия государств – Соглашение между Правительствами государств – членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности. Доступ из справ.-правовой системы «КонсультантПлюс».

26. Соглашение между Правительствами государств – членов Шанхайской организации сотрудничества о сотрудничестве в обла-

сти обеспечения международной информационной безопасности. Доступ из справ.-правовой системы «КонсультантПлюс».

27. Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступностью (вместе с Перечнем компетентных органов государств – участников Содружества Независимых Государств, осуществляющих сотрудничество в борьбе с преступностью) (заключено в г. Москве 25 ноября 1998 г.) // Бюллетень международных договоров. 2000. № 3.

28. Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации (заключено в г. Минске 01.06.2001) // Бюллетень международных договоров. 2009. № 6.

29. Соглашение о сотрудничестве между Российской Федерацией и Европейской полицейской организацией (заключено в г. Риме 06.11.2003) // Бюллетень международных договоров. 2004. № 3.

30. Устав Международной организации уголовной полиции (Интерпол) (с изм. и доп. по состоянию на 01.01.1986) // Национальное центральное бюро Интерпола в Российской Федерации. Москва, 1994.

Специальная литература

1. Актуальные проблемы уголовного права и криминологии: сборник научных трудов кафедры уголовного права / под ред. А. В. Бриллиантова. Москва: РАП, 2014. Вып. 4.

2. *Аносов А. В.* Организационные аспекты виктимологической профилактики преступлений, совершаемых с использованием информационных технологий // Вестник Калининградского филиала Санкт-Петербургского университета МВД России. 2019. № 1 (55).

3. *Антонян Ю. М., Эминов В. Е.* Преступник: основные понятия и черты личности: монография. Москва: Норма: ИНФРА-М.

4. *Биктагирова Г. Ф.* Профилактика и коррекция виктимного поведения студенческой молодежи в Глобальной сети Интернет: теория, практика / Г. Ф. Биктагирова, Р. А. Валеева, А. Р. Дроздикова-Зарипова, Н. Н. Калацкая, Н. Ю. Костюнина. Казань: Изд-во «Отечество», 2019.

5. *Боровская Е. В.* Основы искусственного интеллекта / Е. В. Боровская, Н. А. Давыдова. Москва: Лаборатория знаний, 2018.

6. *Бурыкин А. В.* Криптовалюта как виртуальный инструмент: возможности и недостатки // Перспективы формирования новой экономики XXI века: сборник Международной научно-практической конференции. Актуальные достижения региональной науки. 2017.

7. Виртуальные валюты. Руководство по применению риск-ориентированного подхода. Июль 2015 г. [Электронный ресурс]. URL: http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf (дата обращения: 06.09.2017).

8. Виртуальные валюты: ключевые определения и потенциальные риски в сфере ПОД/ФТ. Отчет ФАТФ. Июнь, 2015.

9. *Волеводз А. Г.* Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. Москва: Юрлитинформ, 2001.

10. Всестороннее исследование проблемы киберпреступности. ООН Нью-Йорк, 2013 г. [Электронный ресурс]. URL: https://www.unodc.org/documents/organized – crime/cybercrime/Cybercrime_Study_Russian.pdf (дата обращения: 15.12.2020).

11. Высокотехнологичная преступность: новые вызовы для общества, государства и бизнеса. [Электронный ресурс]. URL: https://www.pircenter.org/media/content/files/13/14683389400.pdf (дата обращения: 23.07.2019).

12. *Дамаскин О. В.* Криминологические аспекты противодействия преступности: научно-практическое пособие. 2017.

13. Европол – о борьбе по отмыванию денег в криптоиндустрии [Электронный ресурс]. URL: https://bitcoinrush.md/europol-crypto-industria/ (дата обращения: 16.12.2020).

14. Интернет вещей – что это такое и как применять IoT в реальном бизнесе [Электронный ресурс]. URL: https://rb.ru/longread/iot-cards/ (дата обращения: 10.12.2020).

15. Интернет вещей и безопасность инфраструктуры [Электронный ресурс]. URL: https://www.kaspersky.ru/blog/internet-of-things-and-cybersecurity-of-infrastructure/7394/ (дата обращения: 20.01.2021).

16. Интерпол создает свою криптовалюту для борьбы с кибермошенничеством [Электронный ресурс]. URL: http://www.singaporelawwatch.sg/slw/...utm_medium=rss (дата обращения: 08.12.2018).

17. *Ищук Я.Г.* Подготовка специалистов правоохранительной деятельности в сфере борьбы с киберпреступностью // Вопросы совершенствования правоохранительной деятельности: взаимодействие науки, нормотворчества и практики материалы I Ежегодной Всероссийской научно-практической конференции: сборник. 2018.

18. *Ищук Я.Г.* Личность, как объект оперативно-разыскной профилактики преступлений // Оперативник (сыщик). 2017. № 4 (53).

19. *Ищук Я.Г.* Состояние кибервиктимности граждан в контексте обеспечения защиты их основных прав и свобод // Обеспечение прав и свобод человека в деятельности правоохранительных органов: сборник. Рязань, 2018.

20. Как большие данные помогают ловить преступников [Электронный ресурс]. URL: https://media.kasperskydaily.com/wp-content/uploads/sites/90/2015/04/06045539/BD-1024x768.png (дата обращения: 01.11.2019).

21. Кибербезопасность и управление Интернетом: документы и материалы для российских регуляторов и экспертов / отв. ред. М.Б. Касенова; сост. О.В. Демидов и М.Б. Касенова. Москва: Статут, 2013.

22. *Комлев Ю.Ю.* Теории преступности: учебное пособие / Ю.Ю. Комлев; МВД России. Казанский юридический ин-т. 2017.

23. *Кравцов Д.А.* Искусственный разум: предупреждение и прогнозирование преступности // Вестник Московского университета МВД России. 2018. № 3.

24. Криминология и административная юрисдикция полиции: учеб. пособие для студентов вузов, обучающихся по юридическим специальностям / Ю.М. Антонян и др. 2016.

25. *Кудрявцев В.Н.* Причинность в криминологии (О структуре индивидуального преступного поведения): монография. Москва: Норма: ИНФРА-М, 2019.

26. *Кудрявцев В.Н.* Лекции по криминологии: учеб. пособие. Москва: Норма: ИНФРАМ, 2019.

27. *Лапин А.А.* Стратегия обеспечения криминологической безопасности личности, общества, государства и ее реализации органами внутренних дел: монография. Москва: Юнити-Дана, Закон и право, 2017.

28. *Ларина* Е. Умные города и умная полиция – для кого? / Е. Ларина, В.С. Овчинский: https://izborsk-club.ru/15575 (дата обращения: 09.11.2020).

29. *Ларина Е.* Рывок в искусственный интеллект... или фальстарт? [Электронный ресурс] // Е. Ларина, В. Овчинский. URL: https://izborsk-club.ru/16576.

30. *Ларина Е. С., Овчинский В.С.* Искусственный интеллект. Большие данные. Преступность («Коллекция Изборского клуба»). Москва: Книжный мир, 2018.

31. *Ларина Е.С.* Роботы-убийцы против человечества. Киберапокалипсис сегодня / Е.С. Ларина, В.С. Овчинский. Москва: Книжный мир, 2018.

32. *Ларина Е.С.* Криминал будущего уже здесь / В.С. Овчинский, Е.С. Ларина. Москва: Книжный мир. 2018.

33. *Ларина Е.С.* Час волка. Введение в хронополитику / В.С. Овчинский, Е.С. Ларина («Коллекция Изборского клуба»). Москва: Книжный мир, 2019.

34. *Ларина Е.С.* Covid-19: предчувствие апокалипсиса. Хроника окаянной пандемии / В.С. Овчинский, Е.С. Ларина («Коллекция Изборского клуба»). Москва: Книжный мир, 2019.

35. *Ларина Е.С.* Искусственный интеллект. Этика и право. Судья с искусственным интеллектом / В.С. Овчинский, Е.С. Ларина («Коллекция Изборского клуба»). Москва: Книжный мир, 2019.

36. *Ларичев В.Д.* Предупреждение преступлений, посягающих на интеллектуальную собственность: монография / В.Д. Ларичев, Б.Л. Терещенко. Москва: Изд-во «Альфа-Пресс», 2006.

37. Лебедев С.Я. Криминологическая безопасность в системе национальной безопасности России // Российский криминологический взгляд. 2006. № 4.

38. *Лопатин В.Н.* Информационная безопасность России: Человек. Общество. Государство. Санкт-Петербург: Университет МВД России, 2000.

39. *Лунеев В.В.* Эпоха глобализации и преступность / В.В. Лунеев; Институт государства и права РАН. Москва: НОРМА, 2007.

40. *Макаров В.Ф.* Защита информации в телекоммуникационных системах: учеб. пособие / В.Ф. Макаров, А.И. Куприянов; Ака-

демия управления МВД России. Москва: Академия управления МВД России, 2016.

41. Нейротехнологии: нейро-БОС и интерфейс «мозг – компьютер»: монография / В. Н. Кирой, Д. М. Лазуренко, И. Е. Шепелев. Ростов-на-Дону: Южный федеральный университет, 2017.

42. *Овчинский В. С.* Технологии будущего против криминала Москва, Книжный мир, 2017 г.

43. *Овчинский В. С.* Виртуальный щит и меч: США, Великобритания, Китай в цифровых войнах будущего. («Коллекция Изборского клуба»). Москва, Книжный мир, 2018.

44. *Овчинский В. С.* Иностранные боевики-террористы. Иногда они возвращаются. («Коллекция Изборского клуба»). Москва: Книжный мир, 2019.

45. *Овчинский В. С.* Криминология кризиса / В. С. Овчинский. Москва: Норма, 2009.

46. *Овчинский, В. С.* Криминология цифрового мира: учебник для магистратуры / В. С. Овчинский. Москва: Норма: ИНФРА-М, 2018.

47. *Овчинский, В. С.* Основы борьбы с киберпреступностью и кибертерроризмом: хрестоматия / сост. В. С. Овчинский. Москва: Норма, 2017.

48. Ольга Новикова. Европол и Интерпол повысят меры по борьбе с отмыванием денег через криптовалюты [Электронный ресурс]. URL: http://coin-insider.ru/evropol-i-interpol-povysyat-mery-po-borbe-s-otmyvaniem-deneg-cherez-kriptovalyuty (дата обращения: 07.05.2019).

49. ООН и ЮНИСЕФ принимают криптовалюты [Электронный ресурс]. URL: http:// cryptofeed.ru/news/oon-i-yunisef-prinimayut-kriptovalyuty/ (дата обращения: 03.04.2020).

50. ООН назвала криптовалюты «новым рубежом» в мире финансов [Электронный ресурс]. URL: https://forklog.com/oon-nazvala-kriptovalyuty-novym-rubezhom-v-mire-finansov/ (дата обращения: 08.05.2019).

51. Основы информационной безопасности органов внутренних дел: учебное пособие / А. Н. Григорьев и др.; МВД России Департамент государственной службы и кадров. Москва: ДГСК МВД России, 2018.

52. Особенности противодействия киберпреступности подразделениями уголовного розыска: учеб.-метод, пособие / Б. П. Михайлов [и др.]; под ред. Б. П. Михайлова, Е. Н. Хазова. Москва: ЮНИТИ-ДАНА: Закон и право, 2017.

53. Парамонов О. «Большие данные» на службе полиции (и преступников). Доступ из справ.-правовой системы «КонсультантПлюс».

54. *Пинкевич Т.В.* Криминогенные факторы распространения криптоиндустрии в России: сб. материалов Межвузовского круглого стола «Экономико-правовые проблемы использования криптовалюты в расчетах на территории Российской Федерации» 5 апреля 2018 г. Нижегородская академия МВД России, 2018.

55. *Пинкевич Т.В.* Криминологические риски индустрии цифровых технологий в России // Криминальные реалии, реагирование на них и закон (Москва, 23–24 января 2018 г.) / под ред. А.И. Долговой. Москва: 2018.

56. *Пинкевич Т.В.* Легализация криптоиндустрии: за и против // Уголовная политика и правоприменительная практика: сборник статей по материалам V Всеросс. науч.-практ. конференции (3 ноября 2017 г.) / под ред. д-ра юрид. наук, доцента Е.Н. Рахмановой. Филиал ФГБОУВО РГУП, Санкт-Петербург, 2018.

57. *Пинкевич Т.В.* Преступность с использованием криптографических кодов и ее влияние на криминологическую безопасность России // Экономика и право. 2019. № 3.

58. *Пинкевич Т.В.* Проблемы противодействия организованной преступности в сфере цифровой экономики // Борьба с организованными проявлениями преступности и обеспечение национальной безопасности РФ (Москва, 22–23 января 2018 г.): сборник / под ред. А.И. Долговой. М., 2019.

59. *Пинкевич Т.В.* Зарубежный опыт противодействия преступной деятельности с использованием криптовалюты // Научный портал МВД России. 2020. № 3.

60. *Пинкевич Т.В.* Проблемы уголовно-правового противодействия преступной деятельности с использованием криптовалюты // Юристъ-правоведъ. 2020. № 4.

61. *Пинкевич Т.В.* Современное состояние экстремизма и терроризма в условиях развития цифровых технологий / Т.В. Пинкевич, О.А. Зубалова // Юристъ-правоведъ. 2020. № 3.

62. Расследование преступлений в сфере компьютерной информации и высоких технологий: учебное пособие / О.П. Грибунов, М.В. Старчиков. МВД России, Департамент государственной службы и кадров. Москва: ДГСК МВД России, 2017.

63. *Русскевич Е.А.* Уголовное право и «цифровая преступность»: проблемы и решения: монография. Москва: ИНФРА-М, 2019.

64. *Саконян А.* Полиция и большие данные: URL: https://polit.ru/article/2018/06/07/bigdata/ (дата обращения: 18.05.2020).

65. Сборник избранных лекций по криминологии. Москва: Юрлитинформ, 2019.

66. Сборник избранных лекций по криминологии / под ред. Т. В. Пинкевич. Москва: Юрлитинформ, 2020.

67. *Семенюк Р. А.* Криминология: курс лекций / Р. А. Семенюк; МВД России, Барнаульский юридический институт. 2017.

68. Что такое интернет вещей? [Электронный ресурс]. URL: https://lifehacker.ru/internet-of-things-2/ (дата обращения: 05.05.2020).

69. Что такое интернет вещей: существующие технологии [Электронный ресурс]. URL: https://strij.tech/publications/tehnologiya/chto-takoe-internet-veschey.html (дата обращения: 06.10.2020).

Перечень ресурсов информационно-телекоммуникационной сети Интернет, необходимых для освоения дисциплины

1. Информационный сайт института научной информации по общественным наукам Российской Академии наук (ИНИОН РАН) [Электронный ресурс]. URL: http: //www.inion.ru/.

2. Единое окно доступа к образовательным ресурсам [Электронный ресурс]. URL: http://window.edu.ru/.

3. Официальный сайт Правительства России [Электронный ресурс]. URL: http://www.government.ru.

4. Информационный сайт института научной информации по общественным наукам Российской Академии наук (ИНИОН РАН). [Электронный ресурс]. URL: http://www.inion.ru/.

5. Информационный сайт Министерства внутренних дел Российской Федерации [Электронный ресурс]. URL: http: //mvd.ru.

6. Научная электронная библиотека eLibrary.ru [Доступ к РИНЦ (Российскому индексу научного цитирования) и журнальным статьям] [Электронный ресурс]. URL: http://elibrary.ru/.

7. Официальный сайт Президента России [Электронный ресурс]. URL: http://www.kremlin.ru.

8. Информационный сайт Генеральной прокуратуры Российской Федерации [Электронный ресурс]. URL: http://genproc.gov.ru/.

9. Информационный сайт Верховного Суда Российской Федерации [Электронный ресурс]. URL: http://www.vsrf.ru/.

10. Информационный сайт Федеральной службы государственной статистики (Росстат) [Электронный ресурс]. URL: http://www.gks.ru/.

11. Информационно-правовой портал «Гарант» [Электронный ресурс]. URL: http://www.garant.ru.

12. Информационно-правовой ресурс «Консультант Плюс» [Электронный ресурс]. URL: http://www.consultant.ru.

Приложение № 1

Примерные вопросы для подготовки к промежуточной аттестации

1. Цифровая преступность и ее основные свойства (признаки).
2. Основные количественные и качественные показатели цифровой преступности и их характеристики.
3. Социальные последствия цифровой преступности, влияющие на количественные и качественные показатели цифровой преступности.
4. Изучение и использование причин и условий цифровой преступности органами внутренних дел.
5. Понятие и структура личности цифрового преступника.
6. Понятие, объекты и предмет криминологического прогнозирования в эпоху цифровизации общества.
7. Особенности разработки и реализации комплексных программ противодействия цифровой преступности.
8. Классификация мер предупреждения преступлений, совершаемых в цифровой среде по их характеру и масштабу.
9. Субъекты предупреждения цифровой преступности как основной элемент систем и организация их взаимодействия в предупреждении преступлений.
10. Понятие и основные виды обеспечения реализации предупреждения цифровой преступности.
11. Роль правового регулирования предупреждения преступлений, совершаемых в цифровой среде: источники и механизм.
12. Основные направления организационного обеспечения предупреждения цифровой преступности: кадровое, материально-техническое, методическое и др.
13. Понятие и цели информационно-аналитического обеспечения предупреждения цифровой преступности и ее реализации.
14. Информационные ресурсы предупреждения цифровой преступности.
15. Особенности информационно-аналитического обеспечения предупреждения цифровой преступности органов внутренних дел.
16. Понятие преступности в сфере цифровой экономики. Виды цифровой преступности и их классификация.
17. Причины и условия совершения цифровых преступлений. Влияние законодательного регулирования на динамику преступлений в данной сфере.
18. Понятие преступности в сфере цифровых технологий, ее виды, и классификации.

19. Нормативное регулирование отношений в сфере цифровых технологий и организация контроля как основа предупреждения данных преступлений.

20. Понятие преступности в сфере развития и использования технологии больших данных.

21. Причины и условия, способствующие совершению преступлений в сфере развития и использования технологии больших данных.

22. Основные направления предупреждения преступлений, совершаемых в сфере развития и использования технологии больших данных.

23. Понятие преступности в сфере оборота цифровых активов (криптовалюты). Особенности данного вида преступности в современной России.

24. Оценка рисков использования террористами и киберкриминалом криптовалют.

25. Преступления, совершаемые в сфере оборота цифровых активов (криптовалюты).

26. Причины и условия преступлений в сфере оборота цифровых активов (криптовалюты).

27. Проблемы законодательного регулирования и их влияние на динамику преступлений в сфере оборота цифровых активов.

28. Виктимологическая профилактика как основа предупреждения преступлений, совершаемых в сфере оборота цифровых активов (криптовалюты).

29. Понятие преступности в сфере развития и использования искусственного интеллекта.

30. Характерные особенности преступности в сфере развития и использования искусственного интеллекта.

31. Причины и условия совершения преступлений в сфере развития и использования искусственного интеллекта

32. Нормативное регулирование отношений в сфере развития и использования искусственного интеллекта и организация контроля как основа предупреждения данных преступлений.

33. Понятие и виды преступности с использованием IoT (интернет вещей). Понятие интернета вещей.

34. Причины и условия, детерминирующие совершение преступлений с использованием IoT (интернет вещей).

35. Влияние законодательного регулирования на динамику преступлений, совершаемых с использованием IoT (интернет вещей).

36. Основные направления предупреждения преступлений, совершаемых с использованием IoT (интернет вещей).

37. Преступность в сфере интеллектуальной собственности: ее характерные особенности в условиях развития цифровых технологий.

38. Современное понимание экстремистской и террористической деятельности, их общественная опасность и характерные особенности в условиях развития цифровых технологий.

39. Организованный характер экстремистской и террористической и деятельности в условиях развития цифрового общества.

40. Основные направления предупреждения преступлений экстремистской или террористической направленности в условиях развития цифровых технологий.

41. Основные характеристики личности преступников, совершающих преступления преступлений в сфере незаконного оборота наркотических средств и психотропных веществ с использованием цифровых технологий.

42. Организованная преступность: понятие, сущность и особенности ее существования в условиях развития цифровых технологий.

43. Особенности современного изучения организованной преступности.

44. Использование возможностей ООН и других международных организаций в борьбе с цифровой преступностью.

45. Понятие и общая характеристика международных стандартов в области борьбы с цифровой преступностью.

46. Особенности сотрудничества стран СНГ в области борьбы с цифровой преступностью.

47. Деятельность Интерпола по предупреждению цифровой преступности.

48. Особенности реализации международных стандартов в области предупреждения цифровой преступности органами внутренних дел.

49. Обеспечение криминологической безопасности в сфере цифровых технологий. Понятие и виды угроз безопасности в цифровой среде.

50. Компетенция, задачи, возможности органов внутренних дел в сфере защиты цифровой среды от преступности.

Глоссарий криминологических терминов

Большие данные (англ. – big data) – обозначение структурированных и неструктурированных данных огромных объемов и значительного многообразия, эффективно обрабатываемых горизонтально масштабируемыми программными инструментами, появившимися в конце 2000-х годов и альтернативных традиционным системам управления базами данных и решениям класса Business Intelligence.

Высокие технологии (англ. – hightechnology, hightech, hi-tech) – это наиболее новые и прогрессивные технологии современности, такие как микро- и нано- электромеханические системы (MEMS/NEMS), технологии энергосбережения и альтернативная энергетика, биометрика, системы контроля и управления доступом, оборонные технологии и технологии двойного назначения, биотехнологии.

Вычислительное устройство – счетно-решающее устройство, автоматически выполняет одну какую-либо математическую операцию или последовательность их, с целью решения одной задачи или класса однотипных задач.

Доступность информации – состояние информации (ресурсов автоматизированной информационной системы), при котором субъекты, имеющие права доступа, могут реализовывать их беспрепятственно. К правам доступа относятся: право на чтение, изменение, хранение, копирование, уничтожение информации, а также права на изменение, использование, уничтожение ресурсов.

Интернет (англ. – Internet) – всемирная система объединенных компьютерных сетей для хранения, обработки и передачи информации.

Информационная инфраструктура – система организационных структур, подсистем, обеспечивающих функционирование и развитие информационного пространства страны и средств информационного взаимодействия.

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Киберинфраструктура – совокупность людей, процессов (в том числе управляющих), и систем, составляющих киберпространство.

Киберобъект – любой индивидуальный объект или субъект, существующий в киберинфраструктуре.

Киберопасность определяется как опасность, вызванная пребыванием и деятельностью в кибепространстве, включая как прямые атаки на компьютеры, так и следствия неправильных или ошибочных действий пользователей, не уделяющих внимания специальным средствам защиты и правилам безопасной работы в компьютерных сетях.

Компьютер – это устройство или система, способное выполнять заданную последовательность операций.

Компьютерная сеть (вычислительная сеть) — система, обеспечивающая обмен данными между вычислительными устройствами (компьютеры, серверы, маршрутизаторы и другое оборудование).

Компьютерная система – любое устройство или группа взаимосвязанных или смежных устройств, одно или более из которых, действуя в соответствии с программой, осуществляет автоматизированную обработку данных.

Конфиденциальность – необходимость предотвращения разглашения, утечки какой-либо информации. Конфиденциальная информация – информация, являющаяся конфиденциальной, то есть «доверительной, не подлежащей огласке, секретной»; это понятие равнозначно понятиям «тайна» или «секрет».

Криминологический мониторинг – это система социально статистического наблюдения, позволяющая устанавливать показатели преступности, уровень ее латентности, социальные последствия; выявлять ее причины и условия, прогнозировать их развитие в будущем; принимать адекватные государственные и общественные меры по предупреждению преступности и устанавливать их эффективность.

Криминологическое планирование представляет собой элемент социального управления, выражающийся в определении субъектов и объектов предупреждения преступности, поиске наиболее эффективных средств и методов противодействия криминальной среде.

Криминологическое прогнозирование представляет собой научное предсказание основных изменений (тенденций) развития преступности или вероятности совершения уголовно-наказуемых деяний конкретными лицами в обозримом будущем, базирующееся на исследованиях, проводимых научными и практическими сотрудниками.

Моделирование – создание упрощенного образа прогнозируемого объекта, отражающего его существенные свойства (график, диаграмма, формула, схема, таблица и т. п.).

Мониторинг в сфере профилактики правонарушений представляет собой комплекс мероприятий, направленных на получение полной информации о состоянии профилактики правонарушений, о функционировании сложной системы в целях управления ею,

о прогнозировании не только преступности, но и причин и условий, способствующих совершению правонарушений, прогнозированию как угроз, так и криминологических рисков, наблюдению за деятельностью субъектов профилактики правонарушений, определению мнения населения о профилактике правонарушений.

Сквозными технологиями являются большие данные, нейротехнологии, искусственный интеллект, системы распределенного реестра (блокчейн), квантовые технологии, новые производственные технологии, промышленный интернет, робототехника, сенсорика, беспроводная связь, виртуальная и дополненная реальности.

Цифровая экономика – это совокупность общественных отношений, складывающихся при использовании электронных технологий, электронной инфраструктуры и услуг, технологий анализа больших объемов данных и прогнозирования в целях оптимизации производства, распределения, обмена, потребления и повышения уровня социально-экономического развития государства.

Цифровая преступность – это социальное противоправное явление, представляющее собой систему преступлений, совершаемых в сфере цифровых технологий или с их использованием, в том числе включая незаконное завладение и предложение или распространение информации в информационно-телекоммуникационных сетях и в виртуальной среде, дополняющей реальность.

Цифровая система – это такая система, в которой цифровой регулятор используется для управления непрерывным объектом.

Цифровая технология – это дискретная система, которая базируется на способах кодирования и трансляции информационных данных, позволяющих решать разнообразные задачи за относительно короткие отрезки времени.

Цифровое устройство (англ. – digital device) – техническое устройство или приспособление, предназначенное для получения и обработки информации в цифровой форме, используя цифровые технологии.

Цифровые технологии – это дискретная система, которая базируется на способах кодирования и трансляции информационных данных, позволяющих решать разнообразные задачи за относительно короткие отрезки времени.

Экспертная оценка – заключается в обобщении мнений специалистов, основывающихся на большом практическом опыте в сфере правоохранительной деятельности.

Экстраполяция представляет собой распространение выводов, полученных при изучении прошлой и настоящей преступности, на ее будущие тенденции.

Список сокращений

ECPA – Европейская премия по предупреждению преступности.
EUCPN – Европейская сеть по предупреждению преступности.
SCIP – Международная организация конкурентной разведки.
WEF – Всемирный экономический форум.
БПЛА – Беспилотные летательные аппараты.
ВВП – Валовой внутренний продукт.
ВЭФ – Всемирный экономический форум.
ДМС – Дирекция по международному сотрудничеству.
ЕКПП – Европейский комитет по проблемам преступности.
ЕС – Европейский Союз.
ИВОП – Индекс восприятия организованной преступности.
ИГИЛ – Мусульманская организация «Исламское государство Ирака и Леванта».
ИИ – Искусственный интеллект.
ИКТ – Информационно-коммуникационные технологии.
МВД России – Министерство внутренних дел Российской Федерации.
МВФ – Международный валютный фонд.
МОМ – Международная организация по миграции.
МОСЗ – Международное общество социальной защиты.
МОТ – Международная организация труда.
МТО ИГ – Международная террористическая организация «Исламское государство».
НИИ – Научно-исследовательский институт.
НКО – Неправительственная организация.
ООН – Организации Объединенных Наций.
ОПГ – Организованные преступные группы.
РНКП – Европол.
СНГ – Содружество Независимых Государств.
ФБР США – Федеральное бюро расследований.
ФАТФ – Группа разработки финансовых мер борьбы с «отмыванием» денег.
ФЗ РФ – Федеральный закон Российской Федерации.
ФСБ России – Федеральная служба безопасности Российской Федерации.
ЦБ РФ – Центральный банк Российской Федерации.
ЭКОСОС – Экономический и социальный совет ООН.
ЮНЕСКО – Организация Объединенных Наций по вопросам образования, науки и культуры.

Для заметок

Учебное издание

Ищук Ярослав Григорьевич
Пинкевич Татьяна Валентиновна
Смольянинов Евгений Серафимович

ЦИФРОВАЯ КРИМИНОЛОГИЯ

Учебное пособие

Редактор *М. А. Фильчагина*
Верстка *А. А. Мельниковой*

Подписано в печать 26.04.2021. Формат 60 x 84 $^{1}/_{16}$.
Усл. печ. л. 14,18. Уч.-изд. л. 13,00. Тираж 191 экз. Заказ № 17у.

Отделение полиграфической и оперативной печати РИО
Академии управления МВД России.
125993, Москва, ул. Зои и Александра Космодемьянских, д. 8

ISBN 978-5-907187-64-1