Федеральное государственное казенное образовательное учреждение высшего образования «Сибирский юридический институт Министерства внутренних дел Российской Федерации»

Кафедра уголовного права и криминологии

Специальность 40.05.02 Правоохранительная деятельность
специализация № 1 «Оперативно-розыскная деятельность»
узкая специализация «Деятельность подразделений по контролю за оборотом наркотических средств и психотропных веществ органов внутренних дел»

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
по теме:

Криминологическая характеристика и профилактика преступности в сфере высоких технологий

Выполнил:
Слушатель группы П-1602
младший лейтенант полиции
Штангауэр Иван Сергеевич

Решение о допуске к защите:
Допущен к защите
Начальник кафедры уголовного права и криминологии, к.ю.н. доцент
полковник полиции
_____ С.М. Мальков
«6» мая 2021 г.

Руководитель
Доцент
кафедры уголовного права и криминологии, к.ю.н. доцент
подполковник полиции
Федорова Елена Анатольевна

Дата защиты:
«23» июня 2021 г.
Оценка: отлично
Председатель ГЭК
полковник полиции
(специальное звание) _____ (подпись) З. В. Скиба (инициалы, фамилия)

Консультант

Красноярск 2021

Оглавление

ВВЕДЕНИЕ

Современный мир очень сильно изменился. Так, в марте 2021 года был подписан меморандум о создании станции на Луне, ученые из Китая на протяжении девяти лет активно проводят эксперименты по внесению конструктивных изменений в геном человека, а в мировую телекоммуникацию внедряется новый сверхбыстрый способ передачи информации через квантовую сеть. Все эти достижения, несмотря на их кажущуюся незначительность для обычного человека, способны существенно повлиять на жизнь общества в ближайшем будущем.

Если раньше для совершения преступления, преступник пользовался исключительно материальными средствами (ножом, пистолетом, набором отмычек и др.), то на сегодняшний день, с учетом технического прогресса, в арсенал современного злоумышленника вошли вредоносные программы, устройства удаленного доступа к компьютеру, средства скримминга и другие потенциально опасные технологии. Изменились методы и способы совершения традиционных преступлений (наркоторговли, мошенничества, кражи, пропаганды терроризма и др.), а правоохранительные органы всего мира столкнулись с совершенно новым явлением – преступностью в сфере высоких технологий.

Особая опасность данного вида преступности состоит в его массовой распространенности и трансграничном характере. Для пресечения этих преступлений необходимо тесное международное сотрудничество и налаженный обмен информацией между правоохранительными органами. Кроме того, противоправные деяния в сфере высоких технологий способна причинить значительный материальный вред за небольшой промежуток времени.

Особая активность преступности в сфере высоких технологий наблюдается в период борьбы с эпидемией COVID-19. Преступники пользуются введенными ограничениями и широкой оглаской вокруг

пандемии в личных целях: продают поддельные лекарства от коронавируса, совершают кибератаки на важнейшие электронные системы хранения информации в больницах, выманивают данные кредитных карт пользователей и похищают деньги со счетов.

Во всем мире государства стараются выработать собственные методы профилактики данного вида преступности. Неоднократно Президентом Российской Федерации упоминалось о необходимости создания и реализации новых подходов по вопросам обеспечение кибербезопасности.[1]

Существенная роль, занимаемая преступностью в сфере высоких технологий в общей структуре преступности, а также необходимость выработки наиболее эффективных мер борьбы с ней, выявлении особенностей личности киберпреступника, установления причин, условий и факторов её возникновения, обосновывают выбор темы исследования и **актуальность**.

Теоретическая значимость проведенного исследования обусловлена тем, что основные выводы и предложения могут быть использованы в дальнейшем при осуществлении научных разработок, связанных с установлением причин, условий и факторов преступности в сфере высоких технологий, а также выработке соответствующих криминологических и уголовно-правовых мер по ее предупреждению.

Значение выпускной квалификационной работы для теории и практики в деятельности органов внутренних дел и иных правоохранительных органов. По результатам исследования сформулированы выводы и рекомендации, которые могут быть использованы при разработке учебных курсов по криминологии, предупреждении преступлений и административных правонарушений, а также при

[1] Заседание коллегии ФСБ России / Официальный сайт Президента Российской Федерации. URL: http://kremlin.ru/events/president/news/65068 (дата обращения: 21.04.2021).

переподготовке и повышении квалификации действующих сотрудников правоохранительных органов.

Апробация результатов исследования. Выводы и основные положения, сформулированные по результатам исследования структуры личности киберпреступника, были предоставлены автором на XXIII международной студенческой научной конференции «Молодежь, наука и цивилизация».

Говоря о **степени научной разработанности** темы в отечественной и мировой теории, а также практике, следует отметить, что теоретические вопросы преступности в сфере высоких технологий, её криминологическая характеристика и проблемы предупреждения явились предметом исследования в трудах многих выдающихся ученых, таких как С.П. Кушниренко, Д.М. Никерова, А.Ж. Саркисяна, Е.С. Ситникова, О.М. Хохлова, Г.А. Черного, Д.К. Чиркова, Н.Р. Шевко и других.

Объектом нашего исследования выступают общественные отношения, связанные с преступностью в сфере высоких технологий, причинами её возникновения, мерами профилактики и предупреждения, а также местом и ролью личности киберпреступника.

Предметом исследования являются статистические данные о состоянии преступности в Российской Федерации, данные о социально-демографических признаках киберпреступников, научные труды ученых в области противодействия преступности в сфере высоких технологий, мнения специалистов по вопросам кибербезопасности и противодействия киберугрозам, а также имеющаяся нормативно правовая база.

Целью исследования является определение понятия и признаков преступности в сфере высоких технологий, выявление причин преступности в сфере высоких технологий, определение форм и эффективных мер по их устранению и предупреждению.

Задачи исследования:

1. Определить понятие преступности в сфере высоких технологий, выделить значимые признаки.

2. Проанализировать состояние, структуру и динамику преступности в сфере высоких технологий.

3. Определить структуру личности преступника, совершающего преступления в сфере высоких технологий.

4. Установить причины, условия и факторы преступности в сфере высоких технологий.

5. Определить формы и меры профилактического воздействия на преступность в сфере высоких технологий.

Теоретическую основу исследования составляют концептуальные положения, идеи, научные обобщения ученых изучающих преступность в сфере высоких технологий, работы А.Ф. Агарагимовой, В.Р. Анташева, С.Н. Евдокимовой, А.А. Комарова, А.Н. Косенкова, С.Н. Яхъеева и других ученых.

В качестве **методологической основы** исследования были использованы общенаучные эмпирические методы: наблюдение, описание и сравнение. Общенаучные теоретические методы: обобщение, анализ, синтез, индукция и дедукция, системно-структурный и статистический. Частнонаучные методы: корреляционный анализ, юридическо-догматический, социально-психологический и психологический. Специальные методы: изучение материалов судебной практики, изучение личности преступника и анализ уголовной статистики.

Нормативную основу исследования составляют: Конституция Российской Федерации (принятая всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020), действующее федеральное законодательство Российской Федерации, в том числе Федеральный закон Российской Федерации от 27.07.2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее – Закон об информационных технологиях),

Федеральный закон Российской Федерации от 28.12.2010 г. №390-ФЗ «О безопасности», Распоряжение Правительства Российской Федерации от 31.12.2020 № 3704-р Федеральный закон от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» (далее - Закон о цифровых финансовых активах и цифровой валюте), положения проекта «Концепции стратегии кибербезопасности Российской Федерации», вынесенного 29.11. 2013 г. на парламентские слушания в Совет Федерации Федерального собрания Российской Федерации, и другие нормативно-правовые акты.

Структура работы обусловлена целью исследования и состоит из введения, трех глав, состоящих из шести параграфов, заключения и библиографического списка.

1. КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА СОСТОЯНИЯ ПРЕСТУПНОСТИ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ

1.1. Понятие и признаки преступности в сфере высоких технологий

На сегодняшний день в криминологии не существует единого толкования понятия «преступность в сфере высоких технологий». Данный термин ученые рассматривают с разных научных позиций.

Н.Р. Шевко предлагает рассматривать преступность в сфере высоких технологий как совокупность всех традиционных преступлений (мошенничество, сбыт наркотических средств и т.д.) для совершения которых используются информационные технологии.[1]

Д.М. Никеров и О.М. Хохлова под этим понятием понимают совокупность преступлений, совершенных с использованием сложных современных технологий, относящихся к наукоемким отраслям производства или обслуживания.[2]

С учетом многообразия доктринальных мнений, полагаем необходимым сформулировать понятие исходя из основных признаков преступности: социального и правового характера, исторической изменчивости, относительной массовости явления, системности, временной и территориальной определенности.

Как и любой другой вид преступности, преступность в сфере высоких технологий явление социальное, оно неразрывно связано с обществом и теми процессами, которые в нем протекают. Невзирая на тот факт, что большая часть этих преступлений совершается в виртуальной среде, а умысел

[1] Шевко Н.Р. Особенности раскрытия и расследования киберпреступлений: проблемы и пути их решения // Ученые записки Казанского юридического института МВД России. 2016 Т. 1. № 1. 2016. С. 13-16.

[2] Никеров Д. М., Хохлова О. М. Преступления в сфере высоких технологий в современной России // Вестник Восточно-Сибирского института МВД России. 2019. №2. С. 91.

преступников направлен на незаконное получение информации или доступ к электронным денежным средствам, тем не менее жертвами этих деяний остаются люди.

Правовой характер преступности подразумевает определение круга деяний, являющихся противоправными и общественно опасными, согласно действующему уголовному закону. В настоящий момент полный перечень преступлений, которые охватываются понятием преступность в сфере высоких технологий, не установлен. Проблемой выступает неопределенность в трактовке самого понятия «высокие технологии». Что оно означает и насколько широко может рассматриваться? На законодательном уровне определение «высокие технологии» не дается, хотя правовые акты содержат нормы-дефиниции относительно терминов «компьютерная информация», «информационные технологии», «информационно-телекоммуникационная сеть» и т.д. На этот счет ряд научных авторов, одним из которых является С.П. Кушнаренко, придерживаются мнения о том, что термин «высокие технологии» тождественен понятиям «компьютерная информация» и «компьютерная среда».[1] Иное мнение имеют Д.К. Чирков и А.Д. Саркисян, которые связывают высокие технологии с распространением сети «Интернет» и информационно-телекоммуникационных сетей.[2] А.А. Комаров подразумевает под высокими технологиями компьютерную информацию и средства использования информационно-телекоммуникационных сетей.[3]

На наш взгляд, под высокими технологиями следует понимать наиболее новые и прогрессивные технологии современности, относящиеся к наиболее наукоёмким отраслям науки и техники.[4] В связи с этим, понятие «преступления в сфере высоких технологий» будет иметь более широкое

[1] Кушниренко С. П. Методика расследования преступлений в сфере высоких технологий // Конспект лекций, СПб юрид. ин-т Генеральной прокуратуры РФ. СПб. 2007. С. 4-18.
[2] Чирков Д. К., Саркисян А. Ж. Преступность в сфере высоких технологий: тенденции и перспективы // Вопросы безопасности. 2013. № 2. С. 160 - 181.
[3] Комаров А. А. О критериях общественной опасности, преступлений в сфере высоких технологий // Актуальные вопросы права, экономики и управления. 2017. С. 243-245.
[4] Некрасова Н. А., Некрасов С.И. Философия науки и техники: Тематический словарь справочник. Учебное пособие. М.: МИИТ, 2009. С.392

смысловое содержание и не ограничиваться конкретным орудием, способом или средством совершения преступления. Использование обобщающего понятия позволит применять его в дальнейшем для обозначения новых преступных посягательств, появившихся в силу научно-технического прогресса, ответственность за которые предусмотрена разными разделами и главами УК РФ.

Для научного исследования такое толкование понятия является слишком широким. Отсутствие четких границ, определяющих конкретный массив преступности, будет препятствовать его качественному криминологическому анализу и выработке действенных мер профилактики. С учетом этого, в нашей работе под «преступностью в сфере высоких технологий» мы будем понимать совокупность преступлений, совершенных с использованием информационно-телекоммуникационных технологий.

В настоящий момент официальная статистическая отчетность, представленная на официальном сайте Министерства внутренних дел Российской Федерации, включает в эту совокупность следующие группы преступлений:

- преступления в сфере экономики;
- преступления против здоровья населения;
- преступления против общественной нравственности;
- преступления в сфере компьютерной информации;

Историческая изменчивость преступности в сфере высоких технологий обусловлена тем, что посягательства, совершенные с использованием компьютерной информации и информационно-телекоммуникационных сетей возникли относительно недавно (в СССР первое преступление в сфере информационных технологий было совершено в 1979 году.) и развиваются весьма стремительно. Связано это в первую очередь с эволюцией научно-технического прогресса, массовой компьютеризацией общества и внедрением современных цифровых технологий в различные сферы производства.

Как и любой другой вид преступности, преступность в сфере высоких технологий явление массовое. На сегодняшний день совершение подобных общественно опасных деяний нельзя назвать исключением, в преступную деятельность вовлечено множество лиц, обладающих специальными познаниями, которые они используют для реализации преступного умысла. Стоит учитывать, что преступность в сфере высоких технологий – явление относительно массово, нежели абсолютное. Оно носит характер социальной патологии, а, следовательно, не все лица за определенный период времени и на определенной территории, достигшие возраста уголовной ответственности, будут совершать киберпреступления.[1]

Системность преступности в сфере высоких технологий объясняется регулярной повторяемостью, наличием совокупности всех её элементов (преступлений и лиц их совершающих), наличием устойчивой связи между показателями преступности и ей причинами, а также наличием взаимосвязи между самими преступлениями.

Временная определенность преступности в сфере высоких технологий свидетельствует о том, что резкий всплеск компьютерных и информационно-телекоммуникационных преступлений приходится на начало XXI века, с момента внедрения современных технологий в жизнь общества и государства.

При рассмотрении территориального признака, важно отметить, что преступления, связанные с преступностью в сфере высоких технологий, совершаются на всей территории Российской Федерации, независимо от климатических и географических особенностей региона. В некоторых случаях преступность в сфере высоких технологий может иметь транснациональный и трансграничный характер. Связано это с тем, что пределы преступного посягательства в виртуальной среде не ограничиваются границами государства. Киберпреступники распространяют свою

[1] Криминология (Общая часть): учебное пособие. / под. ред. Л. М. Прозументов, А.В. Шеслер. - Томск. 2017. С. 63.

криминальную активность на несколько стран.[1] Кроме того, лица, совершающие преступления в сфере высоких технологий относятся к разным нациям и народностям, виртуальное пространство не принимает во внимание пол и национальную принадлежность личности.

Резюмируя вышесказанное, с учетом рассмотренных признаков, под *преступностью в сфере высоких* технологий следует понимать исторически изменчивое, социальное и уголовно-правовое негативное явление, представляющее собой совокупность противоправных, общественно опасных посягательств, совершаемых на всей территории Российской Федерации с использованием информационно-телекоммуникационных технологий в сфере экономики, общественной безопасности, здоровья населения, нравственности и компьютерной информации, а также лиц их совершающих, возникшее и получившее распространение в начале XXI века, имеющее транснациональный и трансграничный характер.

1.2 Состояние, динамика и структура преступности в сфере высоких технологий

Состояние, динамики и структуры преступности в сфере высоких технологий была изучена на основе данных уголовно-правовой статистики Министерства Внутренних Дел Российской Федерации (далее - МВД РФ)[2].

[1] Шалагин А. Е. Транснациональная преступность: понятие, признаки, меры противодействия // Вестник экономики, права и социологии. 2016. №3. С. 138-141.

[2] В настоящей работе использованы статистические данные МВД России (см.: Состояние преступности в России за январь–декабрь 2016 года. М. 2017; Состояние преступности в России за январь–декабрь 2017 года. М. 2018; Состояние преступности в России за январь–декабрь 2018 года. М. 2019; Состояние преступности в России за январь–декабрь 2019 года. М. 2020; Состояние преступности в России за январь–декабрь 2020 года. М. 2021.)

Показатели состояния преступности в Российской Федерации за 2020 год свидетельствуют об увеличении количества зарегистрированных преступлений, совершаемых с использованием информационно-телекоммуникационных технологий. В настоящее время на 100 тыс. населения приходится 422 подобных преступления и 54 преступника их совершивших.

Согласно статистическим данным МВД РФ за 2020 год было зарегистрировано 510 396 преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, что по сравнению с прошлым годом больше на 73,4%.

Всего за период с 2017 по 2020 год количество зарегистрированных преступлений в данной сфере увеличилось в 5,5 раз (с 92 470 до 510 396 преступлений). Самый большой прирост по сравнению с предыдущим годом наблюдался в 2018 году и составлял 91,6%. Стоит отметить, что за четыре проанализированных года количество преступлений, связанных с использованием информационно-телекоммуникационных технологий стремительно увеличивается. В 2018 году абсолютный прирост преступности составлял 84 794 зарегистрированных преступления, в 2019 году – 201 939, в 2020 году – 417 926. При этом темп прирост остается стабильным (в промежутке от 66,2% до 91,6%).

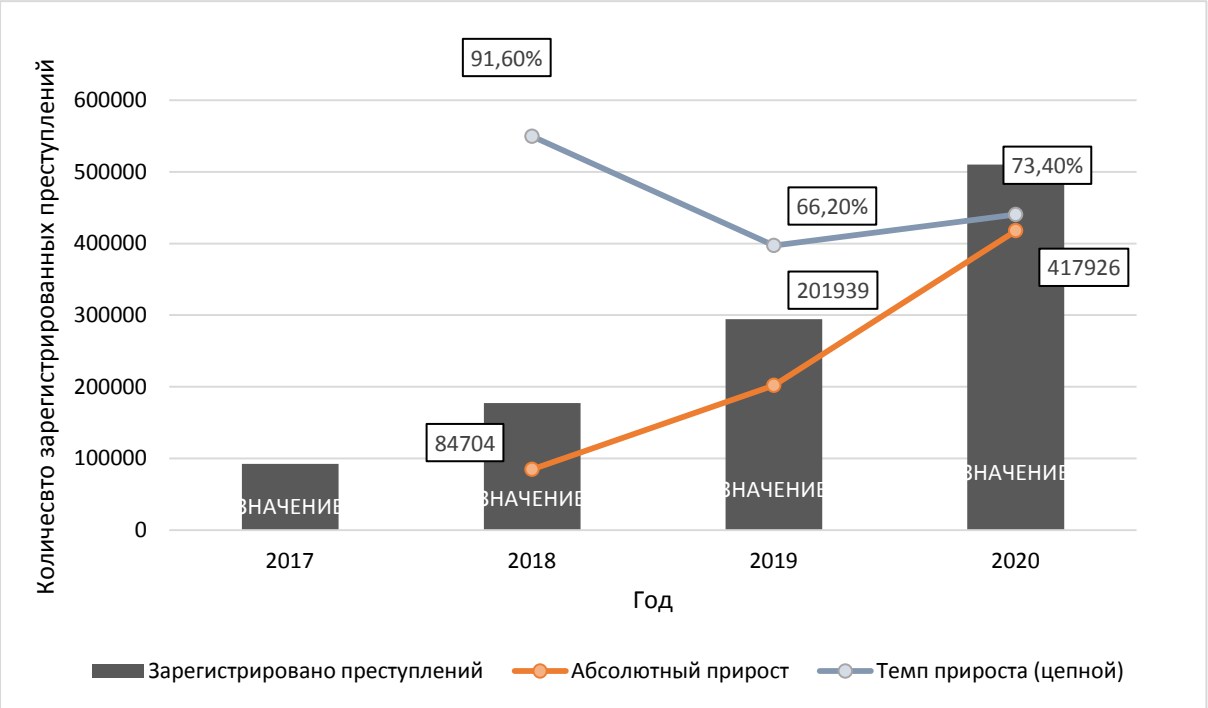
Таблица 1

Преступления в сфере высоких технологий, зарегистрированные в России за 2017-2020 гг.

Годы	Зарегистрировано преступлений	Абсолютный прирост	Темп роста (относительно 2017 г.)	Темп роста (относительно прошлого года)	Темп прироста (относительно 2017 г.)	Темп прироста (относительно прошлого года)
2017	92470	-	-	-	-	-
2018	177174	+84704	1,9	1,9	+91,6%	+91,6%
2019	294409	+201939	3,2	1,7	+218,3%	+66,2%
2020	510396	+417926	5,5	1,7	+451,9%	+73,4%

График 1

Динамика преступности в сфере высоких технологий за 2017-2020 гг.



Далее рассмотрим структуру преступности в сфере высоких технологий за 2019 и 2020 годы. Структура преступности позволяет изучить соотношение отдельных видов преступлений, которые выделяются в зависимости от уголовно-правовых, криминологических или иных смешанных критериев.[1]

Так, наибольшую долю в структуре преступности в сфере высоких технологий занимают преступления в сфере экономики, совершенные с использованием информационно-телекоммуникационных технологий: 80,3% в 2019 году и 80,6% в 2020 году. Каждое третье преступление против собственности в 2020 году было совершено с использованием компьютерных и телекоммуникационных технологий, в 2019 году на долю подобных деяний пришлось каждое четвертое преступление.

[1] Криминология (Общая часть): учебное пособие. / под. ред. Л. М. Прозументов, А.В. Шеслер. - Томск. 2017. С. 67-68.

Преступления против здоровья населения (как правило это сбыт, незаконное производство и пересылка наркотических средств) совершаются реже, в 2020 году их удельный вес составлял 9,2%, в 2019 году этот показатель был равен 8,4%.

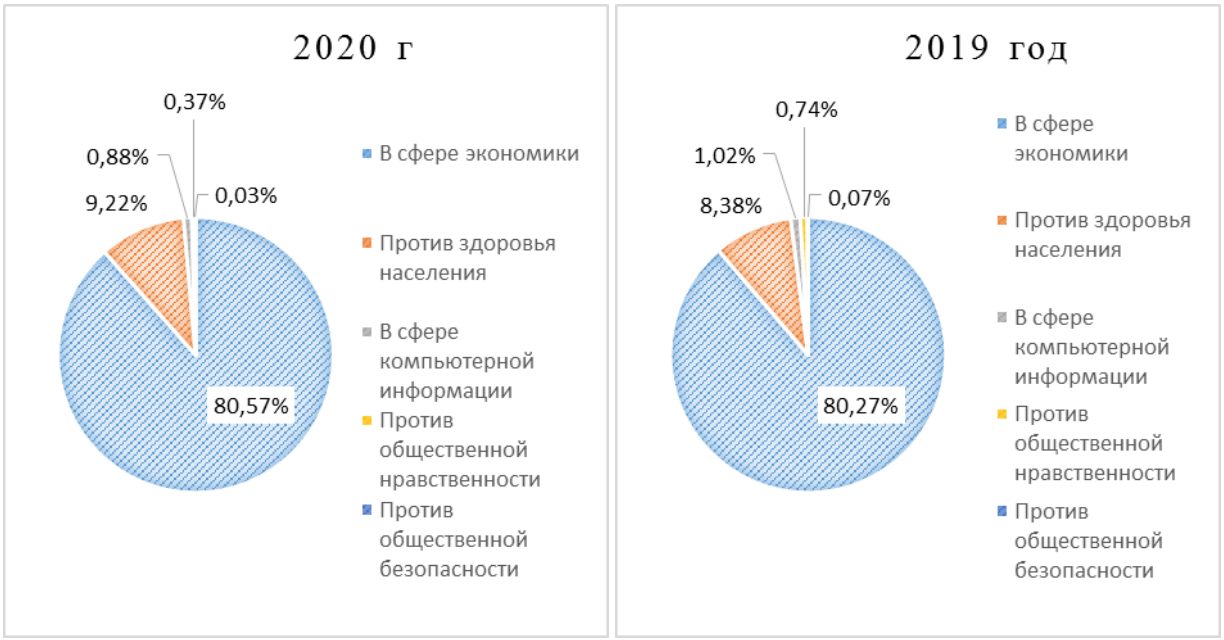
Удельный вес преступлений в сфере компьютерной информации в 2020 году составляет 0,9%, в 2017 году этот показатель был больше на 1,2% что свидетельствует о стабильном снижении данного вида преступлений за прошедших четыре года.

Удельный вес преступлений против общественной нравственности (изготовление порнографических материалов, публичные призывы к осуществлению экстремистской деятельности) равен 0,47% в 2020 году и 0,74 в 2019 году.

В 2020 году удельный вес преступлений против общественной безопасности составлял 0,04%, а в 2019 году 0,07%.

Диаграмма 1

Преступления, совершенные с использованием информационно-телекоммуникационных технологий, за 2019-2020 гг.

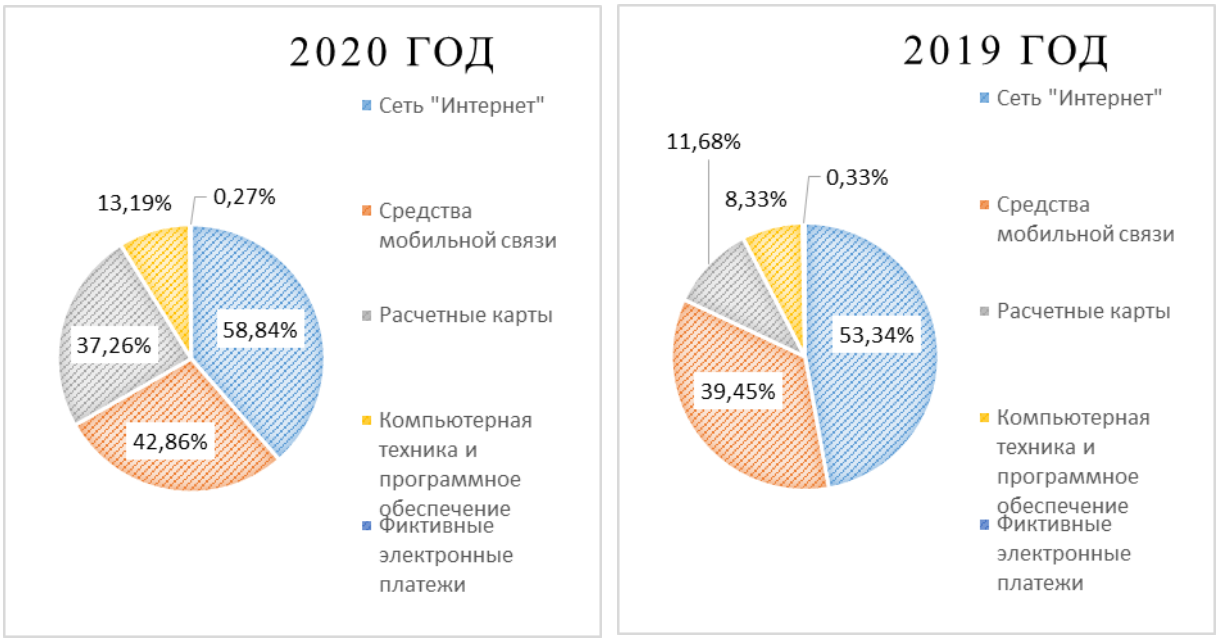


Доля тяжких и особо тяжких преступлений среди преступлений в сфере высоких технологий за 2019 и 2020 год была весьма значительной. В 2019

году она составляла 48,5%, а в 2020 году превысила почти половину от этого показателя и имела значение в 52,4%.

Диаграмма 2

Средства, применяемые для совершения преступлений в сфере высоких технологий в 2019-2020 гг.



Среди средств, используемых преступниками для совершения противоправных деяний в сфере высоких технологий, самым распространенным является сеть «Интернет»: 58,8% (2020 г.), 53,3% (2019 г.). Чуть менее популярны средства мобильной связи: 42,9% (2020 г.), 39,4% (2019 г.). Расчетные (пластиковые карты) имеют удельный вес в структуре равный 37,3% в 2020 году и 11,7% в 2019 году. Прирост за год на 25,6% свидетельствует о повышенном интересе злоумышленников в использовании подобных предметов в своей преступной деятельности. Доля применения компьютерной техники и программного обеспечения не превышает 13,2% (2020 г.), 8,3 % (2019 г.). Самыми незначительным по удельному весу в структуре преступности являются фиктивные электронные платежи, на них приходится 0,27% в 2020 году, 0,33 % в 2019 году.

Таким образом, о состоянии, структуре и динамике преступности в сфере высоких технологий на территории Российской Федерации можно

сделать следующие выводы. Количество зарегистрированных преступлений в сфере высоких технологий стремительно увеличивается. Ежегодный прирост преступлений, связанных с использованием информационно-телекоммуникационных технологий, за период 2017-2020 года составляет более 50%, что говорит о высоких темпах распространения данного вида преступности на территории Российской Федерации. Самыми распространёнными преступлениями, связанными с использованием информационно-телекоммуникационных технологий, являются общественно-опасные деяния в сфере экономики (3/4 от общего количества зарегистрированных преступлений). Наиболее предпочтительными средствами и орудиями совершения подобных преступлений является сеть «Интернет» и инструменты мобильной связи. Отдельной популярностью у злоумышленников пользуются расчетные карты и вредоносное программное обеспечение.

2. ЛИЧНОСТЬ КИБЕРПРЕСТУПНИКА, ПРИЧИНЫ И УСЛОВИЯ СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ

2.1 Личность киберпреступника

Личность преступника понятие социально-правовое. Правовой признак обусловлен совершением лицом общественно опасного деяния с последующим вступлением в уголовно-правовые отношения с государством. Социальный признак представлен в виде совокупности социальных, психологических и биологических качеств, которые выделяют преступника в общей массе. Стоит учитывать, что формируются эти качества, исходя из общественных отношений в которые лицо вступает в процессе своей жизнедеятельности. В связи с этим в криминологии описание преступника происходит благодаря распределению этих отношений по группам, способным в полной мере продемонстрировать структуру личности и её характер.

В нашем случае для изложения криминологической характеристики личности будем придерживаться позиции, в соответствии с которой выделяются три больших блока, формирующих структуру личности (личность, совершающую преступления в сфере высоких технологий мы будем называть киберпреступником, поскольку круг деяний последнего совпадает со сферой использования сети «Интернет», электронных средств платежа, мобильной связи и т.п.):

1. Социально-типологическая характеристика.
2. Социально-ролевая характеристика.
3. Нравственно-психологическая характеристика.

Социально-типологическая характеристика личности киберпреступника основана на принадлежности этой личности к той или

иной социальной группе, которая в свою очередь различается по социально-демографическим признакам (пол, возраст, образование, род занятий) и уголовно-правовой характеристике.

Опорой для нашего анализа станут статистические данные Судебного департамента при Верховном Суде Российской Федерации (далее – Судебный департамент) о состоянии судимости в России[1]. В силу того, что в статистических отчетах Судебного департамента преступления в сфере высоких технологий не выделены в отдельный массив преступности, а определить круг деяний, образующих эту преступность, не представляется возможным, то при анализе нами были учтены только составы преступлений в сфере компьютерной информации. На последующие выводы указанное обстоятельство не повлияет, поскольку демографические признаки личности преступника, совершающего преступления в сфере высоких технологий весьма схожи с признаками личности преступника совершающего преступления в сфере компьютерной информации (обе группы этих преступников реализуют свою деятельность с аналогичным набором специальных знаний).

Для наглядного анализа статистических данных, характеризующих социально-демографические признаки личности киберпреступника, все значения представлены в таблице 2.

Таблица 2

Основные демографические признаки осужденных за преступления в сфере компьютерной информации с 2015 по 2019 гг.

Годы		2015	2016	2017	2018	2019
Всего осуждено	Кол-во	235	185	203	129	165

[1] В настоящей работе использованы статистические данные Судебного департамента при Верховном Суде Российской Федерации (см.: Сводные статистические сведения о состоянии судимости в России за 2015 год. М. 2016; Сводные статистические сведения о состоянии судимости в России за 2016 год. М. 2017; Сводные статистические сведения о состоянии судимости в России за 2017 год. М. 2018; Сводные статистические сведения о состоянии судимости в России за 2018 год. М. 2019; Сводные статистические сведения о состоянии судимости в России за 2019 год. М. 2020.)

Годы		2015	2016	2017	2018	2019
В том числе женщины	Кол-во	9	10	11	16	24
	Уд. Вес (%)	3,8%	5,4%	5,4%	12,4%	14,5%
Возраст						
14-17 лет	Кол-во	0	3	6	3	2
	Уд. Вес (%)	0%	1,6%	2,9%	2,3%	1,2%
18-24 года	Кол-во	93	65	60	42	55
	Уд. Вес (%)	39,6%	35,1%	29,5%	32,5%	33,3%
25-29 лет	Кол-во	72	45	61	31	37
	Уд. Вес (%)	30,6%	24,3%	30%	24%	22,4%
30-49 лет	Кол-во	63	66	71	47	67
	Уд. Вес (%)	26,8%	35,7%	34,9%	36,4%	40,6%
50 лет и старше	Кол-во	7	6	5	6	4
	Уд. Вес (%)	3%	3,2%	2,5%	4,6%	2,4%
Образование						
Высшее профессиональное	Кол-во	70	72	78	42	62
	Уд. Вес (%)	29,8%	38,9%	38,4%	32,5%	37,6%
Среднее профессиональное	Кол-во	88	54	57	42	48
	Уд. Вес (%)	37,4%	29,2%	28,1%	32,5%	29,1%
Среднее общее	Кол-во	62	49	50	35	41
	Уд. Вес (%)	26,4%	26,9%	24,6%	27,1%	24,8%
Основное общее, начальное или нет образования	Кол-во	15	10	18	10	14
	Уд. Вес (%)	6,4%	5,4%	8,9%	7,7%	8,5%
Род занятий						
Рабочие	Кол-во	55	45	42	29	45
	Уд. Вес (%)	23,4%	24,3%	20,7%	22,5%	27,3%
Государственные и муниципальные служащие	Кол-во	3	3	0	3	4
	Уд. Вес (%)	1,3%	1,6%	0%	2,3%	2,4%
Служащие	Кол-во	34	32	45	19	43
	Уд. Вес	14,5%	17,3%	22,2%	14,7%	26,1%

Годы		2015	2016	2017	2018	2019
коммерческой или иной организации	(%)					
Предприниматели	Кол-во	24	17	23	4	11
	Уд. Вес (%)	10,2%	9,2%	11,3%	3,1%	5,4%
Учащиеся и студенты	Кол-во	24	14	14	10	5
	Уд. Вес (%)	10,2%	7,6%	6,9%	7,7%	3%
Военнослужащие	Кол-во	3	5	5	4	1
	Уд. Вес (%)	1,3%	2,7%	2,5%	3,1%	0,6%
Нетрудоспособные	Кол-во	2	2	4	3	3
	Уд. Вес (%)	0,8%	1,1%	2%	2,3%	2,4%
Трудоспособные без постоянного источника дохода	Кол-во	100	73	80	59	53
	Уд. Вес (%)	42,5%	39,5%	39,4%	45,7%	32,1%
Безработные	Кол-во	0	2	1	1	2
	Уд. Вес (%)	0%	1,1%	0,5%	0,8%	1,2%
Сотрудники правоохранительных органов	Кол-во	1	1	1	0	2
	Уд. Вес (%)	0,4%	0,5%	0,5%	0%	1,2%

Преступность в сфере высоких технологий характерна для лиц мужского пола, однако в период с 2015 по 2019 год наблюдается стабильный рост осужденных лиц женского пола. Так, по состоянию на 2019 год соотношение мужчин и женщин составляло 85,5% и 14,5% соответственно, для сравнения в 2015 году это соотношение было равно 96,2% и 3,8%. Причиной складывающейся ситуации, является изменение самовосприятия женщин в современном мире. Сегодня женщины чувствую себя более независимыми: у них появилось стремление реализовывать себя не только в семье, но и вне её пределов. Считается нормой, когда женщина овладевает новой профессии или получает специфические знания, которые ранее были присущи только мужчинам. К примеру, согласно опросу, проводимому в

2019 году компанией Stack Overflow Ltd., женщины составляют 11% разработчиков программного обеспечения. По сравнению с показателями прошлого года это больше на 2%.[1] На фоне развития гендерного равноправия «слабый пол» осваивает в том числе и криминальную среду.[2]

Возраст киберпреступника строго не определен. Самыми криминально активными считаются возрастные группы с 18 до 24 лет (средний удельный вес 34%), с 25 до 29 лет (средний удельный вес 26,3%), а также с 30 до 49 лет (средний удельный вес 34,9%).

При этом, как отмечает И.Ф. Агарагимова, возрастная группа 25-49 лет считается более опасной чем киберпреступники 18-24 лет.[3]

В возрасте 18-24 лет молодые люди только начинают формировать свои навыки работы с вредоносным программным обеспечением. Они не имеют четкого алгоритма преступной деятельности, находятся в поиске новых способов совершения киберпреступлений. Особое внимание мерам конспирации данная категория граждан не уделяет, многие из них не пользуются анонимайзерами (специальные приложения, которые скрывают или меняют местонахождение пользователя при выходе в сеть)[4] или прокси-серверами. С учетом этих особенностей лица в возрасте 18-24 лет, в силу своей юношеской активности и отсутствия опыта, действуют быстро, но неаккуратно, оставляя за своей преступной деятельностью множество следов.

Лица в возрасте от 25 до 49 лет, напротив, имеют за своими плечами большой опыт. К этому возрасту многие из киберпреступников успели поработать системными администраторами, специалистами по

---

[1] Developer Survey Results 2019 // Stack Overflow Limited. URL: https://insights.stackoverflow.com/survey/2019 (дата обращения: 09.02.2021).

[2] Кабайкина О. В., Сущенко О. А. Трансформация роли женщины в современном обществе: в семье и на работе. // Вестник Московского университета. Серия 18. Социология и политология. 2017; Т.23. №3. С. 140-155.

[3] Агарагимова И. Ф. Личность преступника в сфере высоких технологий: сборник научных статей студентов юридического факультета. // Проблемы совершенствования законодательства. 2019. №81/19. С. 83-86.

[4] Ситников Е.С. Закон об анонимайзерах: ответственность за посещение запрещенных сайтов в России. // NOVAUM.RU. 2018. №16. С. 236.

кибербезопасности, тестировщиками программного обеспечения, аналитиками и другими ИТ-специалистами. Преступники в этой группе осознают, что их противоправная деятельность может приносить существенный доход, в связи с чем начинают заниматься ей системно на регулярной основе. Они тщательно продумывают механизмы преступной деятельности, способы противодействия расследованию, легализации доходов и сокрытия своей личности.

Киберпреступники в возрасте 14-17 лет и старше 50 лет считаются наименее криминально активными. Обусловлено это тем, что обе категории граждан еще мало знакомы с принципами функционирования высоких технологий. Единственным отличием между двумя указанными группами служит тот факт, что молодые люди в сравнении с пожилыми людьми наполнены большим энтузиазмом и большими перспективами. Так, в подростковом возрасте несовершеннолетние активно формируют первоначальные криминальные навыки и умения в виртуальной среде, в то время как люди более старшего возраста редко интересуются новыми технологиями и часто не обладают необходимыми ресурсами для обучения.

По уровню образования киберпреступники превосходят остальных осужденных. Согласно статистическим данным Судебного департамента Российской Федерации, наибольшее количество осужденных киберпреступников имеют высшее профессиональное образование (средний удельный вес 35,4%), средним профессиональным образованием обладают 31,3%, средним общим 25,9%. Если говорить о лицах, которые имеют основное общее, начальное образование, либо не имеют образования вовсе, то их количество среди киберпреступников весьма незначительное и в среднем составляет 7,4%. Исходя из представленных данных можно сделать вывод о том, что степень образованности киберпреступников находится на высоком уровне, 2/3 осужденных имеют высшее или среднее образование и только 1/3 окончила школу или не училась вовсе.

Сложившаяся ситуация объясняется наличием необходимости у киберпреступников обладать должным уровнем квалификации и специальными познаниями. Специализация в той или иной сфере позволяет злоумышленникам выбирать наиболее предпочтительный вид и способ совершения преступлений (создание вредоносной программы, мошенничество с использованием пластиковых карт и др.).

В зависимости от рода занятий внушительнее количество киберпреступников относятся к числу трудоспособных лиц без постоянного источника дохода 39,8% (средний удельный вес за пять лет). Среди официально трудоустроенного из числа осужденных наибольшее количество занимают рабочие – 23,3%, затем служащие коммерческой или иной организации – 18,9% и предприниматели – 7,9%. Учащиеся и студенты, согласно данным статистики, имеют весьма незначительную долю среди преступников – 7,1%. Удельный вес остальных групп осужденных, таких как государственные и муниципальные служащие, военнослужащие, сотрудники правоохранительных органов, нетрудоспособные и безработные, составляет менее 1,9%, а значит они весьма редко встречаются среди изучаемого нами вида преступников.

Такое большое количество трудоспособных киберпреступников без постоянного источника дохода обусловлено тем, что эти лица живут исключительно за счет средств, получаемых преступным путем, и редко занимаются официальной трудовой деятельностью.

Удивителен тот факт, что доля студентов и учащихся занимает незначительное место в общей массе киберпреступников, невзирая на общепринятое мнение о том, что молодежь взаимодействует с компьютером гораздо более тесно нежели взрослые. Вероятно, в юном возрасте люди только начинают знакомство с техникой и не готовы в полной мере заниматься преступной деятельностью.

Таким образом, социально-демографический портрет личности киберпреступника представляет собой лицо мужского пола в возрасте от 25

до 49 лет, преимущественно с высшим или средним профессиональным образованием, не занимающиеся официальной трудовой деятельностью.

Для анализа уголовно-правовой характеристики личности киберпреступника мы будем учитывать такие признаки, как вид совершенного преступления, тяжесть, наличие соучастия, судимости и рецидива.

Согласно сведениям о состоянии преступности в Российской Федерации практически каждое второе преступление, совершаемое киберпреступником, является тяжким или особо тяжким.

В Таблице 3 представлены статистические данные Судебного департамента о характеристике преступлений в сфере компьютерной информации по числу осужденных с 2015 по 2019 год.

Таблица 3

Сведения о характеристики преступлений в сфере компьютерной информации по числу осужденных с 2015 по 2019 год

Уголовно-правовые признаки		**2015**	**2016**	**2017**	**2018**	**2019**
Всего осуждено	Кол-во	235	185	203	129	165
Преступление совершено в группе	Уд. Вес (%)	14	12	20	17	34
	Кол-во	6%	6,5%	9,8%	13,2%	20,6%
Преступление совершено в организованной группе	Кол-во	2	2	9	4	14
	Уд. Вес (%)	0,8%	1,1%	4,4%	3,1%	8,5%
Осужденные имели неснятую или непогашенную судимость	Кол-во	11	7	22	13	13
	Уд. Вес (%)	4,7%	3,8%	10,8%	10,1%	7,9%
Наличие рецидива	Кол-во	7	5	11	4	4
	Уд. Вес (%)	3%	2,7%	5,4%	3,1%	2,4%

Свой преступный умысел данные лица реализовывали преимущественно в одиночку, лишь 11,1% осужденных совершали общественно-опасные деяния в составе группы, 3,6% в составе организованной группы. Большая часть осужденных киберпреступников совершают два и более деяние впервые и ранее не привлекались к уголовной ответственности. Только 7,45% осужденных ранее имели неснятую или непогашенную судимость, а у 3,32% в противоправных деяниях признавали рецидив.

Таким образом, уголовно-правовая характеристика киберпреступника имеет следующие отличительные особенности: 1/2 от общего количества совершаемых злоумышленников деяний относится к категории тяжких или особо тяжких преступлений. Киберпреступники редко совершают преступления в группе и, как правило, не имеют непогашенной и неснятой судимости, идут на противоправные действия впервые.

Социально-ролевая характеристика личности киберпреступника формируется исходя из занимаемой им определенной социальной позиции и личного отношения к ней.

В целом о киберпреступнике, исходя из его внешних признаков, создается впечатление законопослушного гражданина (в реальной жизни он придерживается общесоциальных норм морали, успешно выполняет роль ученика, работника, коллеги, соседа и т.п.). В семье это лицо не вступает в конфликты с близкими, поддерживает родственные отношения, но вместе с тем очень скрытен и замкнут. Отсутствие доверительных отношений в родной среде лишает его возможности оградить себя от дальнейшей преступной деятельности. В школе, равно как и на работе, отсутствуют заметные отклонения от норм поведения, киберпреступник не отличается от других, а одноклассники (коллеги) и учителя (руководство) в большинстве случаев не подозревают о его преступной жизни. Как и в семье, преступник замкнут, неразговорчив и раздражителен, особенно когда разговор заходит о его доходах, деятельности в интернете и увлечениях технологиями.

Причиной подобного поведение может быть скрытое «раздвоение личности». Для злоумышленника, занимающегося подобного рода деяниями, существует два мира: реальный и виртуальный. Если в первом мире киберпреступник по тем или иным причинам (отсутствие возможности скрывать свою личность, воспитательный контроль родителей и т.д.) вынужден соблюдать нормы закона и морали, то во втором мире он получает полную свободу действий и мыслей.

В преступной среде киберпреступник старается выделиться на фоне остальных, проявить свою уникальность и преимущество над другими. Положение в криминальной иерархии определяет возможности и сферу влияния в мире высоких технологий.

Если говорить об отношении к труду, то большинство из киберпреступников в качестве основного источника дохода выбирают преступную деятельность в качестве альтернативы работе. Поэтому большинство этих лиц безработные и учащиеся. Иногда киберпреступники все же устраиваются на работу, но делают это в целях маскировки своего противоправного образа жизни.

Досуг киберпреступника проходит за изучением новых правил работы с программным обеспечение, совершенствованием навыков кодирования и криптографии. Большую часть сводного времени эти лица проводят в виртуальном пространстве, но, как и все люди, периодически встречаются с друзьями и близкими, ходят в кино, на вечеринки, ужинают в ресторанах и путешествуют. Общение со знакомыми преимущественно проходит в социальных сетях или мессенджерах.

Нравственно-психологическая характеристика личности отражает отношение преступника к обществу, его мировоззренческие установки, ценностные ориентации и морально-этическую направленность.

Одной из особенностей, отличающей психологическое отношение киберпреступника к совершаемым противоправным деяниям, является особая среда их реализации. В общеуголовной преступности взаимосвязь

между преступником, жертвой и предметом посягательства является прямой. Прямая связь морально усложняет процесс преодоления преступником черты закона. В этом случае объект преступления имеет материальную форму. В случае с преступлениями в виртуальном пространстве во взаимосвязи «преступник-потерпевший (предмет преступления)» включается еще один элемент – электронное устройство. Данный факт создает опосредованное восприятие, что устраняет материальный объект из сознания преступника и создает границу между законными действиями и общественно опасными деяниями неразличимой.

Особое место среди факторов, влияющих на психологию киберпреступника, занимает сетевая анонимность. При этом анонимность означает не только полное отсутствие данных о себе, но и их подмену на те, что были бы более удобными для совершения правонарушений. Имеющаяся конфиденциальность порождает безнаказанность, она в свою очередь вседозволенность, которая замыкает круг и провоцирует киберпреступника на самые опасные и страшные преступления (содействие террористической деятельности, доведение до самоубийства, пропаганда терроризма и другие).

Вместе с тем, на психику киберпреступника накладывается повышенная самоуверенность, осознание своей исключительности, гениальности и неуловимости. Для подтверждения этих убеждений злоумышленники объединяются в сообщества хакеров (крэкеров) – людей, владеющих высоким уровнем специальных знаний в области преступности с использованием программного обеспечения и компьютера.[1]

Определить акцентуацию характера киберпреступника не всегда представляется возможным. Обусловлено это делением у этих лиц мира на две части: на реальное пространство и на виртуальное пространство. Так, в реальном мире злоумышленник может относится к шизоидному типу личности (предельно осторожен и замкнут, находятся в своем закрытом

[1] Криминология: учебник и практикум для академического бакалавриата. / под. ред. Афанасьева О. Р., Гончарова М. В., Шиян В. И. М.: Юрайт. 2018. С. 67

мире, отличается бурными сексуальными фантазиями, недовольством общепринятыми правилами и нормами), а в виртуальном мире, напротив, киберпреступник будет носить признаки истероидного типа личности (излишнее самолюбив, действует демонстративно и стремится выделиться из общей массы).[1] Встречаются также и иные комбинации акцентуации характера.

Мотив преступления является для киберпреступника тем внутренним стержнем, побуждающим его совершить противозаконные действия. Среди мотивов преступлений в сфере высоких технологий выделяют корысть, желание самоутвердиться, деструктивные стремления, протестные настроения, насилие и сексуальная одержимость.

На основе полученных данных о признаках личности киберпреступника и его мотивации, можно выделить следующие типы:

1) По характеру мотивации:

– Корыстный. Это самый часто встречающийся тип киберпреступников. Цель - получение материальной выгоды. Преступная деятельность, связанная с использованием информационно-телекоммуникационных технологий способна компенсировать любую финансовую потребность киберпреступника. Согласно статистическим данным за 2020 интернет-мошенники похитили приблизительно 150 млрд. рублей.[2] Для сравнения, уставной капитал одной из крупнейших компаний России - ОАО «Нефтяная компания «Роснефть», составляет около 105 миллионов рублей[3] (преступный доход мошенников в 1 428 раз больше). При

[1] 28.Юрьева В.Г. Психология преступного поведения и ее зависимость от акцентуации характера преступника // Вестник Таганрогского института имени А.П. Чехова. 2016. №1. URL: https://cyberleninka.ru/article/n/psihologiya-prestupnogo-povedeniya-i-ee-zavisimost-ot-aktsentuatsii-haraktera-prestupnika (дата обращения: 10.12.2020).

[2] Рынок интернет мошенничества в России [Электронный ресурс] // Исследования BrandMonitor. URL: https://media.brandmonitor.ru/rynok-internet-moshennichestva-v-rossii (дата обращения: 10.12.2020).

[3] Устав ПАО «Нефтяной компании «Роснефть». // Официальный сайт ПАО «Роснефть». URL: https://www.rosneft.ru/upload/site1/document_file/rosneft_charter2.pdf (дата обращения: 10.12.2020).

этом, помимо традиционных экономических ценностей (деньги, ценные бумаги и т.п.), предметом посягательства могут быть вещи, имеющие особую ценность для самого киберпреступника или сообщества в которое он входит (игровые призы, награды, достижения т.д.).

– Самоутверждающийся. Лица этого типа стремятся занять наиболее высокое положение в иерархии виртуального социума. Поднятие собственного авторитета - основная целью киберпреступника данной группы. Авторитет позволяет киберпреступнику компенсировать те недостатки, которые у него имеются в реальном мире. Реализация этого мотива происходит путем взлома самых известных интернет-площадок. Так, члены самого известного преступного интернет сообщества «Anonymous», в период с 2008 по настоящее время на регулярной основе проводят крупные интернет-атаки на правительственные сайты, включая сайт Интерпола[1] в феврале 2012 года и сайт Ватикана в марте 2012 года[2]. Объекты взлома подбираются исходя из их роли в социальной, политической и экономической сферах жизни общества и государства.

– Социально дезорганизующий. Часто дополнительным мотивом преступников этого типа может быть желание самоутвердиться. Основная цель – это нарушение социальных и правовых норм, которая реализуется путем дезорганизации органов государственной власти, крупных коммерческих и иных организаций. Так, упомянутая выше атака «Anonymous» на сайт Интерпола была реализована не только с целью удовлетворения самооценки членов группы, но и для выведения интернет-ресурса из рабочего режима, что не позволяло осуществлять международной службе нормальную деятельность.

– Протестный. Киберпреступники, относящиеся к протестному типу, используют информационно-телекоммуникационные и компьютерные

[1] Anonymous вывели из строя сайт Интерпола в ответ на аресты // Lenta. URL: https://lenta.ru/news/2012/02/29/anony (дата обращения: 11.12.2020).

[2] Хакеры из Anonymous атаковали сайт Ватикана // Lenta. URL: https://lenta.ru/news/2012/03/07/vatican/ (дата обращения: 11.12.2020).

технологии с целью участия в идеологической и политической борьбе, а также выражению своих экстремистских взглядов. Учитывая тот факт, что интернет в современном мире стал мощной информационной площадкой, злоумышленники стараются захватить над ним контроль. Сегодня любой пользователь глобальной сети, используя средства сетевой анонимности, может выразить свои политические взгляды и религиозные убеждения, независимо от того наложен на них запрет или нет. В 2005 году Питер Крап описал подобное поведение термином «хактивизм», под которым подразумевал политически конструктивную форму государственного неповиновения или анархический жест[1].

– Насильственный. Мотивы этих лиц связанны со склонением других лиц к совершению самоубийства или причинения увечий. В отличии от традиционных форм совершения этих преступлений, методы и способы, применяемые киберпреступниками, в современном мире изменились. Так, особо популярным способом является создание интернет-сообществ, нацеленных на склонение лица к суициду (одним из таким пример является сообщество «Синий Кит»)[2] и реализации деятельности, именуемой cyberbullying (киберзапугивание) и cyberstalking (киберпреследование). Насилие в этом случае причиняется на расстоянии путем оказания сильного психологического давления на жертву.

– Сексуально озабоченный. Озабоченность этих лиц проявляется в виде побуждения других лиц к действиям сексуального и развратного характера, посредством использования социальных сетей и мессенджеров, а также распространением порнографических материалов.[3] Для

[1] Peter Krapp. Terror and Play, or What was Hacktivism? // Grey Room. MIT Press. 2005. URL: https://www.researchgate.net/publication/238425073_Terror_and_Play_Or_What_Was_Hacktivism (дата обращения: 15.12.2020).

[2] Берг Е. Городская легенда. Что стоит за игрой «Синий кит» и всплеском интереса к «суицидальным пабликам? // Meduza. 2017. URL: https://meduza.io/feature/2017/02/17/gorodskaya-legenda-chto-stoit-za-igroy-siniy-kit-i-vspleskom-interesa-k-suitsidalnym-pablikam (дата обращения: 15.12.2020).

[3] Косенков А. Н., Черный Г. А. Общая характеристика психологии киберпреступника. // Всероссийский криминологический журнал. 2012. №3. С. 92.

киберпреступников этого типа характерны бурные сексуальные фантазии и тяга к развратным действиям, которую удается удовлетворить путем призыва к аморальным действиям в сети.

2) По степени общественной опасности:

– Профессиональные киберпреступники. Считаются самыми опасными, поскольку обладают самым высоким уровнем специальных знаний в области информационно-телекоммуникационных технологий (разработка вредоносного программного обеспечения, знание техники компьютерного взлома, обмана, анонимизации и сокрытия следов).

– Лица, имеющие поверхностные технические знания. Киберпреступники этой группы не способны самостоятельно разработать компьютерный вирус или собрать специальное электротехническое устройство. Как правило, лица данной категории пользуются уже готовыми алгоритмами, программами и техническими приспособлениями. Типичными представителями этой группы являются мошенники, кардеры и распространители порнографических материалов.

– Лица, не обладающие никакими техническими знаниями. Опасность деятельности этих лиц сведена к минимуму. Киберпреступники этого типа могут оказаться живым орудием в руках опытного злоумышленника и быть использованы ими для реализации преступного умысла (снятие похищенных денежных средств с банкомата и передача их непосредственному исполнителю преступления). Не исключены случаи организации такими лицами преступной группы, путем объединения лиц, имеющих специальные знания, для совершения преступлений в сфере высоких технологий.

Таким образом, под киберпреступником, с учетом его отличительных свойств личности, следует понимать - лицо мужского пола в возрасте 25-49 лет, имеющее высшее или среднее профессиональное образование. Отношение к труду у данной категории лиц зачастую негативное, чаще всего киберпреступники предпочитают преступный доход официальному

заработку. Наиболее популярным мотивом совершения преступлений является корысть. Реже встречаются преступники с желанием самоутвердиться, дезорганизовать деятельность государственных органов и иных организаций. Иногда мотивом может выступать потребность в реализации своих протестных, сексуальных или насильственных намерений. Для нравственно-психологических особенностей характерно частое нарушение социальных норм и подмена реального пространства на виртуальное, что в исключительных случаях может приводить к психическим расстройствам, акцентуациям или патологиям.

2.2 Причины преступности в сфере высоких технологий

Одной из главных задач, рассматриваемых криминологией, является установления причин, условий и факторов возникновения преступности. Еще в V веке до нашей эры древнегреческий философ Эмпедокл Акрагантский утверждал: «Ничто не может произойти из ничего, и никак не может то, что есть, уничтожиться». Это высказывание, равно как и упомянутая выше задача, тесно связано с учением о взаимосвязи всех явлений и процессов в мире. Данное учение в философии получило название «детерминизм» – доктрина о всеобщей причинности. В связи с этим, говоря о причинах, криминологи часто используют термин детерминант, что в переводе с латыни означает «определять».

Для более детального рассмотрения причин преступности в сфере высоких технологий мы классифицируем их на три основных уровня: общесоциальный, социально-психологический и личностный.[1]

[1] Криминология (Общая часть): учебное пособие. / под. ред. Л. М. Прозументов, А.В. Шеслер. - Томск. 2017. С. 144.

Общесоциальный уровень детерминант мы разделим на пять групп в зависимости от сфер общественной жизни, которые они затрагивают: политическую, экономическую, социальную, правовую и иные сферы, выделенные в отдельную подгруппу.

Политические причины преступности в сфере высоких технологий включают в себя:

1. Низкий контроль со стороны государства за средствами массовой информации.

Анализируя новостные порталы сети «Интернет» часто можно встретить записи о деятельности киберпреступников или интернет-мошенников. В большинстве подобных сообщений источник новостей, помимо описания самого события преступления, также описывает и механизм его совершения, что служит своего рода инструкцией для читателя. В открытом доступе насчитывается более десятка интернет-сайтов, содержащих подробную информацию о создании вирусного программного обеспечение, изготовлении специальных технических средств или способах взлома систем безопасности. К числу таких сайтов можно отнести www.github.com, www.xakep.ru, www.oszone.net, www.habr.com и др.

Особую опасность эти Интернет-ресурсы несут для несовершеннолетних. В гибком сознании ребенка информация, полученная из такого источника, становится инструментом удовлетворения подростковых потребностей (выделиться среди сверстников, быть самостоятельным, заработать много денег и т.д.), что в последствии приводит к криминальным результатам.

В настоящий момент Роскомнадзор ведет активную деятельность по блокированию нежелательных Интернет-источников. Несмотря на это не всегда в поле зрения данной службы попадают действительно опасные для информационного потребления сайты. С учетом доступности использования Даркнета (скрытой сети внутри интернета, которую не видно обычными

способами) становится очевидным, что подобный контроль за нежелательными Интернет-порталами – мера неэффективная.

2. Использование кибератак в качестве нового вида нападения и защиты.

Традиционно первыми субъектами использования новейших видов оружия традиционно признаются вооруженные силы.

Так, в Китайской армии создано подразделение 61398, задачами которого является обеспечение защиты национальных компьютерных систем, а также совершение нападений на компьютерные системы врага. Подразделение 61398 блокировало уже ни одну атаку на крупнейшие фирмы КНР, но по официальным данным не произвело еще ни одного кибернападения.

Подобное подразделение вооруженных сил есть у Соединенных Штатов Америки, Великобритании, Южной Кореи и России. Невзирая на ограниченный список государств, в которых сформированы кибервойска, многие страны имеют их на неофициальной основе, чем пользуется для совершения политических и военных маневров.

Согласно независимому расследованию газеты New York Times было выявлено, что вредоносная программа Stuxnet была создана при поддержке специальных служб Израиля в целях дестабилизации ядерной программы Ирака в 2011 году.[1]

Распространение кибероружия на международном уровне, создает серьёзную опасность для всего человечества. Так, поступающая на вооружение национальных армий боевая робототехника, управляемая удаленно с помощью программного обеспечения, может быть взломана киберпрестуниками и использована в личных целях.

[1] Broad W. J., Markof J., Sanger D. E. Israeli Test on Worm Called Crucial in Iran Nuclear Delay // The New York Times. 2011. URL: https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html (дата обращения: 22.02.2021).

Экономические причины преступности в сфере высоких технологий представлены в виде нестабильного социально-экономического состояния, провоцирующего злоумышленников обогащаться за счет совершения противоправных действий в виртуальной среде.

Согласно исследованиям швейцарского банка «Credit Suisse» в 2015 году доля среднего класса в России составляла всего 4,1% от всего населения страны. Средним классом признавались лица, имеющие средний годовой доход равный 18 000 USD (примерно 90 750 рублей в месяц по среднему курсу доллара в 2015 году).[1] К 2021 году количество этих лиц существенно не увеличилось.

Исходя из этих данных, можно заметить, что средний класс в Российской Федерации практически отсутствует. Столь кардинальное разделение населения на бедных и богатых создает неблагоприятную криминогенную обстановку. Отсутствие возможности у гражданина удовлетворить свои потребности в силу плохого финансового положения, провоцирует его на получение дохода преступным путем. Совершение имущественных преступлений в сфере высоких технологий позволяет получить крупную сумму денежных средств за очень короткий срок, при этом потратить минимальное количество моральных и физических затрат на реализацию преступного умысла.

Так, в соответствии с приговором Октябрьского городского суда Республики Башкортостан № 1-243/2020 от 29 июля 2020 г. по ст. 159.6. и ст. 272 УК РФ была осуждена гражданка Данилова Е.С., которая являясь специалистом офиса обслуживания и продаж ПАО «Вымпелком» (оператор сотовой связи «Билайн»). Имея навыки работы с программным обеспечением, Данилова умышленно из корыстной заинтересованности осуществила доступ в компьютерную программу «1С», используемую сотрудниками ПАО «Вымпелком» для сервисного обслуживания абонентов.

[1] Global Wealth Report 2015 // Credit Suisse Group. URL: https://www.credit-suisse.com/media/assets/corporate/docs/about-us/research/publications/global-wealth-report-2020-en.pdf (дата обращения: 09.02.2021).

В ней она подделала заявление клиента на замену SIM-карты, произвела перевыпуск SIM-карты, реализовала модификацию компьютерной информации, тем самым получив возможность пользоваться лицевым счетом с находящимися на нем деньгами. После этого в период с 17 января 2020 года по 3 февраля 2020 года регулярно совершала хищения чужих денежных средств с этих кошельков на общую сумму 360 430 рублей.[1]

Приведенный пример является лишь малой частью той преступной деятельности, которая совершается в данной сфере ежедневно. Согласно статистическим данным Центрального банка России за первый и второй квартал 2020 года кибермошенникам удалось похитить денежные средства на сумму 4 млрд. рублей.[2] Очевидно, что альтернатива получение заработной платы легальными путями, в настоящих условиях, не выдерживает никакой конкуренции.

Среди социальных причин преступности в сфере высоких технологий следует выделить стремительное развитие информационно-цифровой среды.

Цифровые технологии, мобильные устройства и социальные сети стали неотъемлемой частью повседневной жизни человека. Согласно отчету, подготовленному компаниями «We Are Social» и «Hootsuite» в 2021 году, 4,66 миллиардов человек во всем мире пользуются Интернетом (59,5 % от общей численности людей на планете). Мобильными телефонами пользуются 5,22 миллиардов человек (68,02 % от общей численности людей на планете). Среднее время, которое проводит человек в интернете составляет около 7 часов в день, 4 часа в среднем человек пользуется телефоном.[3] В Российской

---

[1] Приговор Октябрьского районного суда г. Уфы (Республики Башкортостана) № 1-243/2020 от 29 июля 2020 г. по делу № 1-243/2020 // Судебные и нормативные акты РФ. URL: https://sudact.ru/regular/doc/Nr1KqpqIfTLr/ (дата обращения: 23.01.2021).

[2] На фоне пандемии COVID-19 выросла активность телефонных мошенников и киберпреступников в Интернете // Официальный сайт Центрального банка Российской Федерации. URL: http://www.cbr.ru/press/event/?id=8238#highlight=%D0%BC%D0%BE%D1%88%D0%B5%D0%BD%D0%BD%D0%B8%D0%BA%D0%BE%D0%B2 (дата обращения: 01.03.2021).

[3] Simon Kemp. Digital 2021: Global overview report // DataReportal. URL: https://datareportal.com/reports/digital-2021-global-overview-report (дата обращения: 09.02.2021).

Федерации количество интернет-пользователей составляет около 124 миллионов человек (85% от общего населения России).

Несомненно, процесс мировой компьютеризации внедряет в жизнь общества множество полезных инструментов, но на ряду с позитивным влиянием этого явления, оно оказывает и негативное воздействие. Так, массовое использования информационно-телекоммуникационных сетей позволило создать виртуальную среду, используемую для совершения киберпреступлений. Стремительное развитие высоких технологий сделало меры государственного контроля и безопасности неэффективными, что является одним из криминогенных факторов, стимулирующих киберпреступников к совершению большего количества преступлений. Процесс внедрения новых технологий пропорционален процессу развития киберпреступности. Нет интернета и мобильного телефона – нет интернет-мошенничества.

Юридические детерминанты преступности в сфере высоких технологий включают в себя:

1. Несовершенство российского уголовного законодательства в области борьбы с преступностью в сфере высоких технологий.

На сегодняшний день закреплённые в Уголовном кодексе Российской Федерации (далее - УК РФ) нормы, содержащие признаки составов преступлений, связанных с использованием информационно-телекоммуникационных или компьютерных технологий, подвергаются активной критике со стороны научного мира.

Целым рядом научных авторов, включая Т.М. Лопатину[1] и Н.Ш. Козаева, говорится о необходимости пересмотра норм УК РФ, связанных с мошенничеством в сфере компьютерной информации.

[1] Лопатина Т. М. Проблемы формирования уголовно-правового способа борьбы с компьютерным мошенничеством // Библиотека криминалиста. 2013. № 5. С. 34 - 41.

Учеными отмечается потребность в дополнении УК РФ новыми составами преступлений, отвечающими требованиям современной криминологической ситуации.[1]

Неоднозначность в толковании статей УК РФ, связанных с использованием информационно-телекоммуникационных технологий, а также отсутствие уголовно-правового регулирования в отношении отдельных видов деструктивного поведения является серьёзной проблемой, влияющей на развитие преступности в сфере высоких технологий.

2. Несовершенство судебной практики

Несмотря на достаточно объемную судебную практику по делам о преступлениях в сфере высоких технологий, в процессе рассмотрения уголовных дел по существу, раз за разом возникают ошибки в квалификации преступных деяний. Подобные ситуации необходимо анализировать, обобщать и не допускать в будущем.

На данный момент большинство судов, при рассмотрении подобного рода преступлений назначают киберпреступникам наказание, не связанное с лишением свободы, ссылаясь на то, что деяния такого характера относятся к категории небольшой или средней тяжести.

Так, согласно сведениям о мерах наказания, назначенных осужденным за преступления в сфере компьютерной информации, в период с 2015 по 2019 год, удельный вес лиц, которым было назначено наказание в виде лишения свободы, не превышал показателя в 6,89%.

При вынесении обвинительных приговоров срок лишения свободы заменяют иными видами наказания (штраф, ограничение свободы, условное наказание и тд.).

К примеру, 23 июля 2020 г. Ленинский районный суд г. Оренбурга рассмотрел уголовное дело № 1-538/2020 в отношении Костина М.Ф., который в период с 26 декабря 2019 года по 11 февраля 2020 года незаконно,

[1] Евдокимов К. Н. Основные причины компьютерной преступности в современной России // The Journal of Siberian and Far Eastern Studies. 2014. №8. С.69-70.

из корыстных побуждений, приобрёл и хранил контрафактные экземпляры программных продуктов «1С» общей стоимостью 1 837 700 рублей, с целью их дальнейшего сбыта, а затем незаконно использовал объекты авторского права (осуществил установку копий программных продуктов на компьютер другого лица), то есть совершил деяния, за которые предусмотрено привлечение к уголовной ответственности по п. «в» ч.3 ст.146 УК РФ, ч. 2 ст. 273 УК РФ.

Суд признал Костина М.Ф., виновным в совершении преступления и назначил ему условное наказание в виде лишения свободы сроком на 2 года.

Подобная практика, связанная с недостаточной суровостью назначаемого наказание, будет и в дальнейшем сопутствовать рецидиву со стороны киберпреступников.

К иным причинам преступности в сфере высоких технологий следует отнести:

1. Недостаточную эффективность деятельности следственных и оперативно-розыскных подразделений правоохранительных органов.

Одним из субъектов, занимающихся вопросами раскрытия преступлений в сфере высоких технологий является управление «К» МВД России. Подразделение осуществляет свою деятельность с 1997 года и согласно данным пресс-центра МВД России ежемесячно изобличает киберпреступников в противоправной деятельности. Несмотря на упорную работу сотрудников правоохранительных органов, количество раскрытых управлением «К» преступлений оказывается недостаточным в сравнении с нарастающими объемами преступности в сфере высоких технологий.

Подразделению необходимо расширяться. Для повышения эффективности деятельности подразделения штат сотрудников должен соотносится с актуальным состоянием преступности. В VI века до н.э. китайский военачальник Сунь-Цзы говорил: «Меньшая сила, независимо от перевеса, всегда уступит большей силе.» - это умозаключение остается актуальным и сегодня. Следует помнить, что преступный мир в виртуальном

пространстве состоит из множества правонарушителей, объединенных общими целями и задачами. Оказать необходимое сопротивление этим лицам будет способен только состав из такого же множества специалистов правоохранительных органов.

Особое внимание стоит уделить профессиональной квалификации сотрудников. Долгое время отдел «К» укомплектовывался оперативными сотрудниками, проходившими службу, связанную с расследованием экономических преступлений, противодействию распространению нелицензионных программ, фильмов, видеоигр и другой компьютерной информации. Очевидно, что упомянутые лица имеют недостаточную подготовку и навыки, необходимых для раскрытия современных киберпреступлений. Полицейский управления «К» должен обладать узкоспециализированным образованием, необходимой квалификации, умениями и навыками в области компьютерных технологий. Важно учитывать специфику каждого вида преступления и подбирать служащих в соответствии с их специализацией (программист, техник в области информационная безопасности, специалист в форензике и др.)

Создание в России киберполиции, которое анонсировал заместитель Министра внутренних дел Российской Федерации Игорь Зубов, возможно и решит указанные проблемы, но так или иначе создание подобной структуры займет продолжительное время.[1]

2. Небезопасность виртуальных сервисов финансовой системы.

Упрощение систем получения услуг через электронные сервисы не только облегчило жизнь граждан и организаций, но и принесло ряд негативных факторов.

Так, введение ПАО «Сбербанк» возможности оформления договора кредитования через онлайн-сервис спровоцировало целую волну преступлений, связанных с хищением денежных средств с банковских карт.

[1] Буркина В. Что такое хорошо? // Щит и меч. 2020. №48. URL: https://xn--b1aew.xn--p1ai/upload/site1/document_journal/Schit_i_mech__48_2020_skleyka.pdf (дата обращения: 01.03.2021).

Мошенники представлялись сотрудниками банка, входили в доверие к гражданам и получали доступ к их персональным данным. После этого, с использованием этих данных, они оформляли кредит на лицевой счет жертвы и похищали денежные средства путем их перевода.

Облегченная процедура кредитования, состоящая из трех основных этапов (заполнение заявки на сайте, получение одобрения в срок от двух минут до двух дней, получение денег онлайн в день одобрения заявки), а также усеченные требования к заемщику (возраст от 18 до 20 лет, стаж работы от 6 месяцев) открыли перед преступниками новый способ хищения денежных средств.

С марта 2021 года ПАО «Сбербанк» запустила виртуального ассистента «Салют», позволяющего переводить денежные средства голосовой командой, при этом подтверждение операции происходит также голосом.[1] Никакой верификации голоса пользователя в этой системе нет, а безопасность, со слов разработчика сервиса К.И. Круглова, обеспечивается только за счет ограничений в сумме перевода.[2] К слову, вопрос о том, как быть с систематическими переводами небольших сумм денег, так и не был затронут, хотя данное упущение может стать новым способом совершения преступлений в сфере высоких технологий. Введение подобных систем и сервисов должно проходить через оценку возможных рисков, но, к сожалению, в настоящее время вопросы выгоды стоят выше проблем преступности.

Технический директор Qrator Labs Артем Гавриченков, который уже более десяти лет занимается защитой информационных ресурсов от кибератак, заявил о том, что зачастую часть внедряемых банком мобильных сервисов не согласовываются с отделом безопасности, либо навязывается

---

[1] Салют, Сбер! Переведи деньги // Официальный сайт ПАО «Сбербанк». URL: https://www.sberbank.ru/ru/person/promo/perevody-salut (дата обращения: 13.03.2021).

[2] Делюгин Е. Про сравнения с «Яндексом», нужды людей и захват рынка ассистентов: рассказывает конструктор техники от «Сбера» // VC.RU. URL: https://vc.ru/story/160830-pro-sravneniya-s-yandeksom-nuzhdy-lyudey-i-zahvat-rynka-assistentov-rasskazyvaet-konstruktor-tehniki-ot-sbera#security (дата обращения: 13.03.2021).

специально. К примеру, получив отказ от отдела безопасности трижды, отдел развития продуктов направляет запрос четвертый и пятый раз, до того момента пока не получит одобрения.[1] Наступившие в результате этого неблагоприятные последствия, связанные получением клиентами убытков, на ответственность банка не влияют. Согласно пользовательскому соглашению приложения «Сбербанк Онлайн» действует принцип «as is», используемый для отказа от некоторых подразумеваемых гарантий на предмет продажи, в силу чего банк не несет ответственности практически за все действия, даже если банку было известно о возможности такого ущерба.

3. Высокая латентность киберпреступлений.

Возможность избежать уголовного преследование, в силу отсутствия у правоохранительных органов информации о преступлении, побуждает киберпреступников продолжать свою противозаконную деятельность.

Большая часть деятельности киберпреступника анонимна. Потерпевшая сторона порой даже не догадывается о преступных посягательствах на её конфиденциальную информацию (персональные данные аккаунтов, номера счетов и т.д.). В отличии от бумажных носителей компьютерная информация никуда не пропадает и не исчезает.

В некоторых случаях потерпевшая сторона (чаще всего это коммерческие организации) и вовсе не желает сообщать о факте совершения общественно-опасного деяния. Так, примером подобного поведения может служить отказ коммерческой организации публично признать себя потерпевшей стороной, мотивируя это тем, что данное заявление может отрицательно сказаться на репутации фирмы, либо раскрыть их собственную незаконную деятельность.

Набирают популярность частные компании, занимающиеся расследованием киберпреступлений. Пользование услугами подобных организаций, в качестве альтернативы правоохранительным органам, создает

[1] Кошкина Ю. Голосовой помощник Сбербанка может подсказывать мошенникам // Дайджест вкладчика. 2019. №110/948. URL: https://www.zvi2015.ru/article/1087 (дата обращения: 13.03.2021).

искусственную латентность, оставляя большое количество преступлений без внимания. Одной из таких организаций является «Group-IB». Она обеспечивает защиту крупнейших российских и зарубежных компаний от финансовых потерь и вреда репутации.

Исходя из вышеперечисленного, можно сделать вывод о том, что причинами преступности на общесоциальном уровне в политической сфере жизни общества является низкий контроль за средствами массовой информации и нежелательными ресурсами сети «Интернет», а также заинтересованность вооруженных сил ведущих стран в создании кибероружия и киберармии. Экономические причины обусловлены нестабильностью экономической обстановки в государстве и негативному влияния кризиса на население. Социальные причины связаны с высоким уровнем компьютеризации населения. Правовыми причинами являются несовершенство уголовного законодательства и судебной практики. Среди иных причин преступности в сфере высоких технологий выделяется слабая защищенность финансовых сервисов, а также недостаточная эффективность деятельности следственных и оперативных подразделений. Кроме того, имеются проблемы, связанные с высокой латентностью преступлений, совершенных с использованием информационно-телекоммуникационных технологий.

Далее мы рассмотрим детерминанты преступности в сфере высоких технологий на социально-психологическом уровне.

Человек на протяжении всей своей жизни является членом той или иной социальной группы. Каждая из этих групп способна оказывать на личность определённое воздействие: позитивное, нейтральное, либо негативное.

Наиболее популярными социальными группами, способными сформировать в личности криминальные черты являются семья, школа и друзья.

Процесс непосредственного влияние семьи на личность будущего киберпреступника происходит чаще всего в форме отсутствия контроля за деятельностью ребенка в процессе формирования его личностного «я». Чтобы контролировать общение ребенка в сети «Интернет» родители как минимум должны обладать базовыми компьютерными навыками, но с учетом возрастных особенностей, имеющейся нагрузки в быту и приверженности к консервативным взглядам, складывается закономерный вывод о том, что реализовать эту задачу могут лишь небольшое число матерей и отцов. В связи с этим родитель, неосознанно, упускает важный этап в развитии ребенка.

Помимо семьи значительное социальное воздействие на личность оказывает школа или иная образовательная организация.

Среднее время нахождения молодого человека в школе или любой иной образовательной организации составляет 5-6 часов в день, что равняется примерно 1/3 времени бодрствования. В связи с этим, определение социально-психологических причин преступности в сфере высоких технологий, возникающих в школе, является обязательным условием криминологического исследования.

В настоящее время школа, как один из самых мощных институтов социализации, выполняет свои функции не в полном объеме. Ребенок, находясь на занятиях, остается предоставленным самому себе, педагоги не имеют возможности уделять воспитанию обучающихся особое внимание и дополнительное время, что способствует еще большему отчуждению ребенка от нормального общества и приобщению к криминальным и деструктивным группам («хакерам»).

Малые социальные группы, сформированные на основе общих интересов (друзья), являются самыми значимыми социальными институтами для формирования личности киберпреступника. За общением с друзьями человек проводит большую часть своего свободного времени. Если коммуникативные связи лица чаще всего возникают в среде

правонарушителей, то со временем изменяется система ценностей и принципов человека. Он становится частью группы, перенимает ее идеи, взгляды и установки. Наиболее подверженными такому давлению являются люди с гибкими жизненными установками. Именно эти лица представляют особый интерес для террористических и экстремистских организаций при вербовке.

Для анализа причин преступности в сфере высоких технологий на личностном уровне рассмотрим механизм индивидуального преступного поведения киберпреступника, который обуславливается нравственно-психологическим состоянием личности во взаимодействии с объективными условиями и обстоятельствами.

И.Я. Козаченко выделяет в механизме индивидуального преступного поведения пять основных этапов: мотивации, планирования, «волимости», исполнения и посткриминальный этап. [1]

На этапе мотивации устанавливаются потребности киберпреступника материального, познавательного, социального, идеологического или сексуального характера. В зависимости от потребностей формируется мотив. К числу наиболее распространенных мотивов преступлений в сфере высоких технологий относят: корысть (алчность, стяжательство), желание повысить свой авторитет в глазах других людей, политические и мировоззренческие мотивы, тяга к насилию и сексуальная одержимость.

После определения мотива преступления наступает этап планирования. На этапе планирования злоумышленник определяет конечную цель, оценивает обстановку, в которой предполагает действовать, выбирает объект посягательства, способы и средства достижения цели, оценивает собственные возможности.

Желаемый результат, которого стремится достичь киберпреступник, зависит от мотива и может выступать в виде обогащения, причинения вреда

[1] Криминология: учебник и практикум для бакалавриата и специалитета / под. ред. Козаченко И. Я., Корсаков К. В. М.: Юрайт. 2019. С. 132.

жизни и здоровью другому лицу, удовлетворения сексуальных желаний, обретения популярности и авторитета, дестабилизации органов государственной власти и др. Иногда совершение преступления может быть самоцелью, что присуще лицам, совершающим хулиганские действия.

Обстановка совершения преступлений в сфере высоких технологий часто представлена в виде виртуального пространства. В связи с этим, в отличии от иных видов преступлений, взаимосвязь между преступником и жертвой становится опосредованной. Это негативно сказывается на жертве, исключает ее бдительность, а также приносит преимущество преступнику, позволяя ему более успешно приспособиться к изменяющимся условиям.

Выбор объекта посягательства обусловлен техническими возможностями и навыками киберпреступника. Как правило определяются наименее защищенные и уязвимые электронные системы, наиболее доверчивые люди.

Способы и средства совершения преступлений в сфере высоких технологий отличаются своим многообразием и вариативностью. Развитие технического прогресса регулярно открывает перед преступниками новые технологии для совершения преступлений (Криптовалюта, виртуальная переадресация абонентским номеров и др.). При этом, при выборе способа совершения преступления злоумышленники в области высоких технологий стараются действовать в обход существующим социальным институтам, либо вопреки им.

При оценке киберпреступником собственных возможностей характерна чрезмерная уверенность в высоком уровне своего интеллекта и специальных знаний. Высокая самооценка провоцирует лицо на совершение преступлений более тяжкой категории. Злоумышленник остается до последнего уверен, что не оставит за собой не единого следа, который мог бы изобличить его.

Следующим этапом в механизме индивидуального преступного поведения является этап «волимости». На этой стадии запланированное преступление согласуется с волей лица.

Особенность указанного процесса в сознании киберпреступника характеризуется тем, что в силу опосредованности восприятия оно не способно адекватно оценивать нанесенный своими действиям вред и последствия.

Профессор Джон Сулер описал эту особенность термином «The Online Disinhibition Effect» (эффект онлайн дезингибиции), который оказывает на активного пользователя интернет-пространства значительное психологическое воздействие.[1] Эффект онлайн дезинибиции включает явление «дисассоциативной анонимности», сущность которого состоит в том, что личность, находясь в условиях анонимности не способна отличать свои действия от действий в реальном мире, а, следовательно, у таких людей пропадает чувство ответственности.

После этапа, связанного с принятием окончательного решения, наступает этап исполнения преступного акта.

В процессе совершения преступления киберпреступник находится в комфортных условиях, поскольку не оказывается привязанным к местоположению объекта преступного посягательства. Внешние факторы, негативно влияющие на лицо в момент совершения преступления (место и время, физико-химические свойства объекта, метеоусловия и др.), отсутствуют или оказываются сведены к минимуму.

На посткриминальном этапе киберпреступник анализирует совершенное деяние.

В процессе анализа эти лица редко испытывают чувство раскаяния или вины. Отсутствие прямой взаимосвязи с жертвой и недостаточная оценка причиненного вреда исключают отражение в сознании

[1] John Suler. The Psychology of Cyberspace // Department of Psychology Science and Technology Center Rider University. URL: http://users.rider.edu/~suler/psycyber/psycyber.html (дата обращения: 25.02.2021).

киберпреступника противоправной деятельности. Напротив, после исполнения запланированного акта у него появляется приятное ощущение удовлетворения.

Учитывая вышеперечисленное, можно сделать вывод о том, что среди основных детерминантов преступности в сфере высоких технологий на личностном уровне можно выделить отсутствие у киберпреступников чувства раскаяния и ответственности за совершенные противоправные действия. Для данной категории лиц характерна повышенная самооценка и уверенность в собственных действиях. В совокупности со всеми остальными признаками, самоуверенность создает такую психологическую среду для преступника, в которой он становится абсолютно свободным и независимым от закона.

Таким образом, преступность в сфере высоких технологий обусловлена сразу несколькими причинами, которые можно условно разделить на три основных уровня: общесоциальный, социально-психологический и личностный. Среди политических причин общесоциального уровня стоит отметить низкий контроль государства за средствами массовой информации, развитие киберподразделений в вооруженных силах. Экономические причины обусловлены отсутствием финансовой стабильности в стране. Социальные причины связаны с ростом количества пользователей информационно-телекоммуникационных сетей и современных компьютерных технологий. Проблемы правового характера включают в себя несовершенство уголовного законодательства и судебной практики. К иным причинам можно отнести латентность, низкую эффективность деятельности правоохранительных органов и небезопасность мобильных сервисов банка. Социально-психологический уровень причин преступности в сфере высоких технологий обусловлен отсутствием должного контроля за воспитанием со стороны семьи и школы. При проведении досуга имеется риск быть подверженным негативному влиянию со стороны окружающих. Детерминанты личностного уровня связаны с

механизмом индивидуального преступного поведения и проявляются в виде неблагоприятной обстановки совершения преступлений (виртуального пространства), тщательного планирования преступных действий, выбора наиболее уязвимых и слабозащищенных объектов посягательства, широкого спектра средств и способов совершения преступления и высокой самооценки лиц их совершающих. Кроме того, особое влияние оказывает возможность оставаться анонимным в сети, отсутствие чувства ответственности и раскаяния за свои действия.

3. ОБЩИЕ И СПЕЦИАЛЬНЫЕ МЕРЫ ПРЕДУПРЕЖДЕНИЯ ПРЕСТУПНОСТИ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ

3.1 Общие меры предупреждения преступности в сфере высоких технологий

Предупреждение преступности является одной из самых важных категорий криминологии, которая представлена в виде многоуровневой системы государственных и общественных мер, ориентированных на устранение и сдерживание причин, условий и факторов преступности.

Традиционно для реализации превентивных мер в отношении наиболее распространенных видов преступности Правительство Российской Федерации совместно с Федеральным собранием Российской Федерации разрабатывает стратегию борьбы с ними. По вопросам противодействия преступности в сфере высоких технологий подобной стратегии нет.

В 2013 году в Совете Федерации Российской Федерации состоялись парламентские слушания, посвященные проекту Концепции стратегии кибербезопасности. По итогам слушаний было принято решение вынести на обсуждение в Интернете указанный проект, но в связи с имеющимися разногласиями с государственной политикой стратегия так и не была утверждена.[1]

Помимо попытки создания внутригосударственных правовых актов в 2017 году Российская Федерация представила в Генеральную Ассамблею ООН «Проект Конвенции Организации Объединенных Наций о сотрудничестве в сфере противодействия информационной преступности». На сегодняшний день данный проект конвенции окончательно не одобрен.

[1] Проект Концепции стратегии кибербезопасности Российской Федерации // Совет Федерации Федерального Собрания Российской Федерации. URL: http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf (дата обращения: 05.03.2021).

Учитывая отсутствие правовых основ предупреждение преступности в сфере высоких технологий, в нашей работе мы будет опираться на положения федерального закона «Об основах системы профилактики правонарушений в Российской Федерации» от 23.06.2016 N 182-ФЗ, доктрину информационной безопасности Российской Федерации (утв. Президентом РФ от 09.09.2000 N Пр-1895), проекты упомянутых выше стратегии и конвенции, доктринальные мнения и взгляды.

Для детального рассмотрения мер предупреждения киберпреступности, постараемся упорядочить их на отдельные группы.

В науке предлагаются различные классификации мер предупреждения преступности. К примеру, В.Б. Вехов и В.Е. Козлов разделяют все меры на три основные группы: правовые, организационно-технические и криминалистические.[1] По мнению Т.М. Лопатиной меры должны иметь комплексный характер и быть представлены с одной стороны в виде организационно-управленческих и технических мер, а с другой — в виде кадровых и правовых мер.[2]

Несомненно, с приведенными позициями можно согласиться, но, на наш взгляд, в основу классификации следует положить зависимость от целевого назначения. В соответствии с ним следует различать общие (политические, экономические, социальные, научно-технические, духовно-культурные, виктимологические) и специальные меры предупреждения преступности.

Общие меры предупреждения преступности направлены в первую очередь на достижение общесоциальных задач. Большинство общих мер предупреждения преступности сформулированы в стратегии национальной безопасности Российской Федерации (утв. Президентом РФ от 31.12.2015 № 683).

---

[1] Лопатина Т. М. Криминологические и уголовно-правовые основы противодействия компьютерной преступности: дис. ... док. юрид. наук. - М. 2007. С. 418.

[2] Компьютерные преступления: Способы совершения и раскрытия / под. ред. Вехова В. Б., Смагоринского Б. П. - М. : Право и Закон, 1996. С. 182.

Среди общеполитических мер предупреждения преступности в сфере высоких технологий стоит выделить защиту конституционного строя, сохранение гражданского мира, политической и социальной стабильности в обществе, а также защита населения и территорий от чрезвычайных ситуаций природного и техногенного характера.

К примеру, пандемия COVID-19 спровоцировала рост киберпреступности в России практически на ¼ от прежнего количества зарегистрированных преступлений. Сложная эпидемиологическая обстановка, финансовый кризис, перевод сотрудников на удаленный режим работы, сокращение персонала сформировали для киберпреступников благоприятные условия для противоправной деятельности.

Стоит помнить, что возникновение подобных чрезвычайных ситуаций дезорганизует государственные органы власти и общество в целом, любое происшествие на политической арене предоставляет шанс потенциальным преступникам воспользоваться ситуацией для реализации своих корыстных, протестных, насильственных и иных преступных намерений.

Общеэкономические меры должны быть направлены на поддержание национальной экономики и формирование условий экономического роста. Сильная экономика – основа сильного государства.

Согласно сравнительному анализу показателей социально-экономического развития Российской Федерации в 2008 и 2020 гг., проводимому Институтом комплексных стратегических исследований, темп роста ВВП в стране снизился с 7,9% до 1,3%. Российская экономическая политика держит курс на ограничение экономического роста во имя сохранения «макроэкономической стабильности». Соблюдение подобного подхода позволяет сохранить лидирующие позиции на мировой арене и исполнять поставленные задачи в рамках экономической стратегии.

Так, в соответствии с «Концепцией долгосрочного социально-экономического развития Российской Федерации до 2020 года» фактическая

реализации снижения добычи полезных ископаемых (нефти и газа) соответствует целевым ориентирам.

Однако, стоит учитывать тот факт, что объем накопленных государством нефтегазовых доходов относительно 2008 года снизился в 2,3 раза. Одна из причин сложившейся ситуации - снижение цен на нефть на мировом рынке.

Учитывая приведенные обстоятельства, Российской Федерации необходимо продолжать экономическую политику, направленную на снижение зависимости от нефтегазового сектора, и перераспределение бюджета на развитие человеческого капитала. Ориентация на человеческий капитал позволит повысить уровень образования, медицины, развития технологий, науки и иных отраслей, что в дальнейшем исключит целый ряд причин преступности, связанных с низким уровнем качества жизни населения, недостаточным финансовым обеспечением институтов общества и государства.

Общие меры предупреждение киберпреступности социального характера связаны с улучшением качества жизни граждан. При этом, приоритетной задачей является устранение социального неравенства между бедными и богатыми слоями населения. Государству необходимо обеспечить доступность жилья, высокое качество товаров и услуг, а также достойную оплату трудовой деятельности.

Изменения, внесенные в ст. 133 Трудового кодекса Российской Федерации, связанные с установлением зависимости минимального размера оплаты труда (далее – МРОТ) от величины прожиточного минимума (далее – ВПМ), значительно улучшили социальную ситуацию в стране. Тем не менее особое влияние продолжает оказывать тот факт, что ВПМ не находится в прямом соотношении с уровнем инфляции. Данное обстоятельство серьёзно сказывается на уровне жизни населения и, на фоне низкой эффективности обеспечения социальных гарантий граждан, провоцирует их всё чаще выбирать преступные способы обогащения. Именно поэтому наиболее

популярным мотивом среди киберпреступников является корысть, «корни» которой вероятнее всего заложены отсутствием реальной возможности подняться по «социальной лестнице» легальными методами.

Исходя из изложенного, предлагается и дальше вносить изменения в законодательство и совершенствовать систему социальных гарантий. Введенная с 1 января 2021 года новая методика исчисления МРОТ является примером наиболее эффективного пути социально-экономического развития России. Хочется верить, что она оправдает себя и повлияет на финансово-материальное положение граждан и, как следствие, на преступность.

Научно-технические меры предупреждения заключаются в активизации фундаментальных и прикладных научных исследований, развитии перспективных высоких технологий, а также повышении качества подготовки научных работников.

Помимо этого, стоит уделить особое внимание расширению сети федеральных университетов, специализирующихся на подготовке будущих специалистов кибербезопасности и инновационных технологий. В научных организациях должны быть созданы специализированные группы ученых, занимающихся исследованием киберугроз и уязвимых мест «даркнета».

Ярким примером эффективности использования научных трудов и помощи образовательных организации в расследовании преступлений в сфере высоких технологий стал опыт Федерального бюро расследования Соединенных Штатов Америки. В 2014 году исследователи из университета Карнеги-Меллон смогли взломать сеть Tor и получить данные реальных IP пользователей сети, которые в последствии были использованы для блокирования преступной торговой интернет-площадки «Silk Road» и задержания её организатора Росса Уильяма Ульбрихта.[1]

Стоит отметить, что подобное взаимодействие научных центров и правоохранительных органов встречается и в Российской Федерации.

[1] Chris Mills Judge Confirms Carnegie Mellon Hacked Tor and Provided Info to FBI // Gizmodo. URL: https://gizmodo.com/judge-confirms-carnegie-mellon-hacked-tor-and-provided-1761191933 (дата обращения: 07.03.2021).

Так, согласно данным British Broadcasting Corporation Федеральная служба безопасности Российской Федерации периодически осуществляет заказы у частных компаний в сфере передовых технологий и научно-исследовательских институтов.[1]

Кроме того, летом 2020 года на базе Санкт-Петербургского политехнического университета Петра Великого был создан Институт кибербезопасности и защиты информации.

В структуре Московского Университета Министерства внутренних дел Российской Федерации имени В.Я. Кикотя существует факультет подготовки специалистов в области информационной безопасности, который с 2002 года готовит будущих сотрудников Бюро специальных технических мероприятий МВД России. С 2017 года данный факультет обеспечивает реализацию программ высшего образования по узкой специализации «Оперативно-техническое обеспечение раскрытия и расследования киберпреступлений», первый выпуск обучающихся по данной образовательной программе запланирован на 2022 год.[2]

В образовательных организациях ФСБ России имеется факультет информационной безопасности, входящий в академию ФСБ России[3], а также Московский институт новых информационных технологий ФСБ России, который готовит будущих преподавателей, а также осуществляет повышение квалификации действующих сотрудников правоохранительных органов.[4]

---

[1] Сошников А. Рейтер С. Москит, Надежда, Наутилус: хакеры раскрыли суть проектов тайного подрядчика ФСБ // BBC News. URL: https://www.bbc.com/russian/features-49050982?fbclid=IwAR39d-JCwHnEQg7mHXFwwqChe7bwxu1bhuyIzgoHA16yqxwMbgINDbxk-38 (дата обращения: 07.03.2021).

[2] Факультет подготовки специалистов в области информационной безопасности // Московский Университет МВД России имени В.Я. Кикотя. URL: https://inlnk.ru/W403P (дата обращения: 21.03.2021).

[3] Факультет информационной безопасности // Федеральная служба безопасности Российской Федерации. URL: http://academy.fsb.ru/i_faculty_ib.html (дата обращения: 21.03.2021).

[4] Информация о деятельности Московского института новых информационных технологий ФСБ России // Официальный сайт Московского института новых

В будущем, по мере развития данных образовательных учреждений, научные исследования студентов, аспирантов и преподавателей могут стать хорошим подспорьем в борьбе с преступностью в сфере высоких технологий в России.

К духовно-культурным мерам предупреждения преступности в сфере высоких технологий следует отнести развитие в современном обществе положительных духовно-нравственных ценностей, прививание идеи гуманизма и недопустимости аморального поведения, формирование уважения к национальным и семейным традициям.

Компьютеризация населения, опосредованное общение между людьми, возникшее вследствие использования мессенджеров и социальных сетей, размывает имеющиеся социальные нормы и правила. Нравственные устои традиционного общества сменяются новыми принципами виртуальных идеологий и течений. Учитывая тот факт, что современный человек проводит в интернете 7 часов бодрствования из 16, государству необходимо принять серьезные усилия, направленные на сохранение верных представлений о допустимом поведении, о добре и зле, о патриотическом воспитании и других духовных ценностях.

Сегодня духовная и культурная сфера должны распространять свое влияние не только в реальном мире, но и в среде Интернет-пространства. Борьба за внимание компьютерного пользователя является одной из приоритетных задач институтов культуры, средств массовой информации и социально-полезных общественных объединений. Так уж сложилось, что «запретный плод» всегда был «слаще» для человека, поэтому превентивные меры духовно-культурного характера должны в полной мере покрывать негативное воздействие высоких технологий на население.

информационных технологий ФСБ России. URL: http://minit.fsb.ru/minit/information.htm (дата обращения: 21.03.2021).

В отдельную группу следует отнести виктимологические меры предупреждения преступности в сфере высоких технологий. В число виктимологических мер входит:

1. Активизация профилактического воздействия средств массовой информации на граждан пожилого возраста.

Согласно статистическим данным Mediascope среднесуточная аудитория канала "Россия 1" в крупных городах составила 1 миллион 338 тысяч человек, у «Первого канала» 1 миллион 128 тысяч зрителей, у «НТВ» 1 миллион 10 тысяч телезрителей.[1] При этом во время рекламной паузы у экранов, в среднем, остается около 50 % аудитории.[2] С учетом того, что целевой аудиторией телевидения являются люди пожилого возраста, использование этого периода для демонстрации профилактических роликов захватит большую часть населения страны, подвергнутой действиям мошенников.

Помимо телевидения, также следует обратить внимание на крупные видео-хостинги (YouTube, Vimeo, Rutube и др.). Современная тенденция показывает, что молодые люди предпочитают смотреть кино, развлекательные передачи, документальные сюжеты и другие виды видеоматериалов в интернете, поэтому в этой среде также важно развивать предупреждение киберпреступности.

Содержание профилактических роликов должно в доступной форме информировать о наиболее распространенных методах мошенничества с использованием высоких технологий. Объяснять порядок действий граждан в случае совершения в отношении их подобных деяний. Кроме того, на наш взгляд, с целью воздействия на потенциальных киберпреступников необходимо демонстрировать в роликах жертв преступлений, которые так и

[1] Рейтинги телевидения // Mediascope. URL: https://mediascope.net/data/ (дата обращения: 20.03.2021).
[2] Назайкин А. Медиапланирование на телевидении // Бизнес-Ключ. 2007. № 1. URL: https://www.bkworld.ru/archive/y2007/n01-2007/n01-2007_182.html (дата обращения: 20.03.2021).

не смогли вернут свои деньги. Истории таких лиц будут служить предупредительным примером для граждан, а также демонстрировать последствия преступлений, которые не могут быть восприняты киберпреступниками в силу опосредованности восприятия.

2. Информирование молодежи о роли высоких технологий в жизни общества и ответственности за их неправомерное использование.

Очень важно сформировать у несовершеннолетнего лица верное представления о предназначении и целях создания современных технологий.

Прежде чем допускать ребенка к использованию «Интернета», следует предварительно подготовить его к этому: рассказать его структуру, проинформировать о том какие материалы ребенку разрешается просматривать, а какие стоит игнорировать. Важно объяснить причины этих правил, зачем законодателем ограничена та или иная деятельность и к чему она может привести (при этом стоит упоминать не только об уголовной ответственности, но и об общественном вреде, наносимом такими деяниями).

Вместе с тем, молодым людям стоит прививать основы кибербезопасности, объяснять важность антивирусного программного обеспечения, способы защиты конфиденциальных данных и правила обращения с банковскими картами. Помимо обучения естественным и базовым дисциплинам, ученикам в школе должны разъясняться основы поведения в обществе и взаимодействия с административными органами.

Так, с 2012 года Министерством внутренних дел Российской Федерации проводится акция «Безопасный Интернет», целью которой является повышение подготовленности пользователей к безопасной работе в Интернете. В рамках акции сотрудники полиции проводят интерактивные уроки, рассчитанные на школьников 11-14 лет. Особое внимание на таких занятиях уделяется необходимости соблюдения морально-этических норм в онлайн-общении и методах противодействия кибербуллингу.

3. Внесение в перечень российских программ для предустановки на продаваемые в России смартфоны, компьютеры и телевизоры с поддержкой Smart TV защитного программного обеспечения.

31 декабря 2020 года Правительство Российской Федерации утвердило перечень российских программ для предустановки на продаваемые в России смартфоны, компьютеры и телевизоры с поддержкой Smart TV. В их число вошли «Почта Mail.ru», «Госуслуги», «Яндекс.Диск» и другие. Среди всех программ, включенных в перечень, только программа Kaspersky Internet Security является тем приложением, которое направлено на обеспечение кибербезопасности пользователя. При этом, устанавливаться данная программа будет только на телефоны и телевизоры с операционной системой Android, тем самым оставив в стороне пользователей телефонов от Apple Inc. и компьютеров на базе Windows, Mac OS и Linux.

На наш взгляд целесообразно было бы расширить список приложений, обеспечивающих безопасность.

Среди рекомендуемых программ для предустановки на электронные устройства стоит отметить «Who Calls» от Лаборатории Касперского. Данное приложение определяет входящий номер, тем самым предупреждая о спаме и нежелательных номерах. Количество бесплатных функций в этом приложении ограничено и для полного доступа необходима подписка. Несмотря на незначительную стоимость подписки (129 рублей в месяц) стоит отметить, что не каждый гражданин России может себе её позволить, поскольку потребность, связанная с защитой от киберугроз часто удовлетворяется в последнюю очередь. Считаем, что необходимо наладить договоренность с компанией о предоставлении бесплатного доступа к расширенной базе данных и функциям приложения, хотя бы на период всплеска интернет-мошенничества в стране.

4. Увеличение банком сроков обработки переводов денежных средств.

В настоящие время срок перевода денежных средств на дебетовую карту банка занимает от 1 минуты до 24 часов в зависимости от способа совершения платежа.

К примеру, ПАО «Сбербанк» для зачисления переводов по фамилии, имени, отчеству и номеру телефона, а также по номеру карты тратит всего несколько минут. Для переводов по номеру счета срок составляет от 30 минут до 5 дней.

При этом, стоит еще раз отметить, что время обработки перевода зависит только от способа его совершения. Важно, что банком никак не учитывается размер денежных средств, пересылаемых другому клиенту банка.

Находим разумным создать внутри банков механизм зависимости срока обработки денежных операций от суммы перевода, что позволит в случае оперативного обнаружения мошеннических действий оспорить перевод в банке и отменить его, сохранив денежные средства у владельца.

Несомненно, введение данного механизма значительно скажется на мобильности переводов, в связи с чем ввести применение подобных ограничений целесообразно только от суммы денежных операций, превышающих 250 000 рублей.

Важно учитывать, что не всегда перевод будет единоразовым. Часто мошенники просят жертву осуществить несколько переводов на незначительные суммы (2 000 - 5 000 рублей). В этом случае увеличение срока обработки платежа следует вводить при превышении установленного размера денежных средств за определенный период (сутки, неделя и тд.).

5. Внедрение нового способа идентификации клиентов банка при совершении ими финансовых операций.

История знает множества способов установления личности конкретного человека: от подписи, до уникального папиллярного узора пальцев рук.

Сегодня большинство банков для подтверждения электронных платежей и переводов используют сотовые номера клиентов для направления в их адрес уникального кода. Как показывает практика подобный метод имеет ряд серьезных пробелов в вопросах безопасности и конфиденциальности. Зачастую мошенники просят продиктовать жертву уникальный код, высланный банком, тем самым санкционируют финансовую операцию, которую проводят в тайне от владельца карты.

Современные разработки предлагают человечеству более совершенные способы идентификации. Для примера к таковым можно отнести технологию Touch ID, которая позволяет использовать отпечаток пальца для установления личности пользователя. Каждый отпечаток пальца уникален, поэтому вероятность совпадения даже мельчайших областей разных следов пальцев рук в Touch ID крайне мала. Она составляет всего 1:50 000 для одного сохраненного отпечатка.

Помимо распознавание папиллярных узоров можно идентифицировать человека по лицу (технология Face ID). В данном случае используют ИК-камеры и датчиков глубины, что исключает возможность обмануть систему, поднеся к ней фотографию или показав 3D-маску.

Главной проблемой в применении данной меры является тот факт, что далеко не каждый гражданин страны обладает техническими возможностями для применения таких технологий. Тем не менее, отказ от использования банками уникального набора чисел в пользу технологий распознавания отпечатка пальца или лица, побудит население к обновлению своих электронных устройств на более современные модели, которые будут способны обеспечить необходимый уровень защиты.

Таким образом, к общим мерам предупреждения преступности в сфере высоких технологий следует отнести сохранение конституционного строя и внутригосударственной стабильности, формирование готовности к наступлению чрезвычайных ситуаций, а также недопущение наступления кризисной ситуации внутри страны. Помимо этого, важное значение имеет

развитие внутренней и внешней экономики, смена ее приоритетных направлений, связанных в первую очередь с развитием человеческого капитала. Среди общих социальных мер предупреждения необходимо отметить устранение социального неравенства, повышение уровня жизни населения, создание условий для доступного жилья, продуктов питания и жизнедеятельности. Разработка новых технологий и создания площадки для развития фундаментальных и прикладных научных исследований позволит использовать их достижения для обеспечение цифровой и информационной безопасности общества и государства. Общие духовно-культурные меры должны сохранить нравственные ценности населения в период всеобщей компьютеризации, влекущей искажение в сознании человека действующих социальных норм. К числу виктимологических мер следует отнести активизацию профилактической деятельности средств массовой информации, правовое просвещение и информирование молодежи, увеличение сроков переводов денежных средств через банки, а также внедрение новых способов идентификации клиентов банка.

3.2 Специальные меры предупреждения преступности в сфере высоких технологий

Специальные меры предупреждения преступности включают в себя мероприятия, направленные на непосредственное решение выявленных проблем борьбы с преступностью. В отличии от общих мер, направленных на исполнение стратегических и глобальных задач, специальные меры принимаются исходя из конкретной криминологической ситуации с целью устранения или минимизации ее криминогенного воздействия.

Рассматривать специальные меры предупреждения преступности в сфере высоких технологий мы будем исходя из деления на общую и индивидуальную профилактику.

К специальным мерам общей профилактики преступлений в сфере компьютерной информации можно отнести:

1. Развитие международно-правового сотрудничества по вопросам борьбы с преступностью в сфере высоких технологий.

Трудности по вопросам международного сотрудничества возникают в связи с расхождением позиций различных государств, относительно подходов к определению базовых понятий. Так, Организацией Объединенных Наций был отклонен Проект Конвенции ООН о сотрудничестве в сфере противодействия информационной преступности, разработанный Россией в связи с иной трактовкой понятия информационная преступность.

С учетом трансграничного и транснационального характера преступности в сфере высоких технологий государствам необходимо приходить к общим компромиссам и унифицировать правовые нормы при регламентации действий сторон в процессе использования средств противодействия киберпреступности.[1]

Вместе с этим, важную часть международного сотрудничества составляет деятельность международных организаций.

Для примера, в 2015 году Интерпол инициировал открытие Международного центра по борьбе с киберпреступностью. Двумя года ранее, в 2013 году начал работу Европейский центр по борьбе с киберпреступностью, который за первый год своей работы провёл порядка 20 успешных операций против мошенничества в Сети, взлома сайтов финансовых учреждений и распространения детской порнографии.

[1] Атнашев В. Р., Яхъеева С. Н. Международное сотрудничество в борьбе с киберпреступностью и кибертерроризмом // Евразийская интеграция: экономика, право, политика. 2019. № 3. С. 37-42.

Правоохранительные органы Российской Федерации должны находиться в тесном взаимодействии с данными учреждениями, с целью обмена глобальным передовым опытом по борьбе с преступностью в киберпространстве.

2. Вынесение Верховным судом Российской Федерации (далее – ВС РФ) постановления с разъяснениями о практике рассмотрения судами уголовных дел по преступлениям, связанным с использованием информационно-телекоммуникационных технологий.

На сегодняшний день пленумом ВС РФ вынесен целый ряд судебных решений, направленных на толкование норм УК РФ и устранение проблем, связанных с квалификацией отдельных видов преступлений. Тем не менее до сих пор не было представлено разъяснений о практике рассмотрения судами уголовных дел по преступлениям, связанных с использованием информационно-телекоммуникационных технологий.

С учетом нарастающего объема преступности в данной сфере необходимость в вынесении подобного решения становится всё более актуальной. Данные судом уточнения позволят исключить значительные трудности в правильной квалификации киберпреступлений и привести практику применения уголовно-правовых норм правоохранительными органами и судами к единообразному виду.

3. Введение уголовной ответственности за создание, использование и продажу, специальных систем для удаленного использования электронных устройств.

Одним из примеров подобной системы является компьютерная сеть «Botnet», состоящая из устройств зараженных вредоносной программой. Она используется для организации DDoS-атак, подбора паролей методом Брутфорса (полного перебора), майнинга биткоинов или других криптовалют, а также распространения спама.

Использование подобной системы – это один из самых распространенных методов совершения преступлений в сфере компьютерной

информации, поскольку он позволяет пользоваться чужими ресурсами для достижения своих преступных целей. Тем не менее запрета на создание, использование и продажу систем типа «Botnet» в настоящий момент не существует. В связи с этим считаем необходимым рассмотрение вопроса о включении в уголовный закон подобной нормы.

4. Блокирование сотовой связи на территории учреждений, исполняющих уголовные наказания в виде лишения свободы, и мест содержания под стражей.

В соответствии с пояснительной запиской к законопроекту № 876381 «О внесении изменений в отдельные законодательные акты Российской Федерации в части прекращения оказания услуг связи на территории следственных изоляторов и учреждений, исполняющих уголовные наказания в виде лишения свободы» в 2018 году в учреждениях уголовно-исполнительной системы было изъято 56 249 ед. средств связи.

Сотовые телефоны используются осужденными для организации «колл-центров», из которых они осуществляют звонки гражданам, с целью хищения чужого имущества путем обмана или злоупотребления доверием.

Для решения этой проблемы Российская Федерация воспользовалась опытом Гондураса и обязало операторов сотовой связи отключать мобильную связь на территории учреждений, исполняющих уголовные наказания в виде лишения свободы, и мест содержания под стражей. Отключение происходит на основании письменного решения руководителя регионального управления Федеральной службы исполнения наказаний Российской Федерации (далее –ФСИН России) в случае выявления факта использования осужденными абонентских номеров подвижной радиотелефонной связи.[1]

[1] Федеральный закон от 09.03.2021 № 44-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации в части прекращения оказания услуг связи на территории следственных изоляторов и учреждений, исполняющих уголовные наказания в виде лишения свободы" // Официальный интернет-портал правовой информации. URL:

Выявляются эти номера в процессе проведения оперативно-технических мероприятий с применением специализированного оборудования радиомониторинга.

Данное нововведение уже принесло положительный результат. Так, директор ФСИН России Александр Калашников на заседании коллегии по итогам 2020 года заявил, что благодаря этой процедуре сотрудникам службы удалось выявить и заблокировать более 27 тыс. абонентских номеров.

Для совершенствования этой меры в будущем можно применить технологию «Managed access system». Данная технология работает как маломощная вышка сотовой связи, она принимает вызовы и передает их операторам сотовой связи. Благодаря этой системе абонентский номер можно блокировать сразу, как только злоумышленник попробовал сделать звонок. При этом будет разрешена связь с утвержденными устройствами (мобильными телефонами сотрудников ФСИН России) и службами экстренной помощи.

Специальные меры индивидуальной профилактики могут включать:

1. Постановку лиц, совершающих преступления в сфере компьютерной информации, на профилактический учет.

В соответствии с положениями Федерального закона от 23 июня 2016 г. № 182-ФЗ «Об основах системы профилактики правонарушений в Российской Федерации» профилактический учет, является одной из форм профилактического воздействия, предназначенной для информационного обеспечения деятельности субъектов профилактики правонарушений, направленной на выявление и устранение причин и условий, способствующих совершению правонарушений, а также на оказание воспитательного воздействия на лиц в целях недопущения совершения ими правонарушений или антиобщественного поведения.

---

http://publication.pravo.gov.ru/Document/View/0001202103090043?index=0&rangeSize=1 (дата обращения: 23.03.2021).

Киберпреступникам, наравне с другими категориями граждан, совершающими общественно опасные деяния, очень важно привить верное представление о законопослушном поведении. С этой целью правоохранительные органы должны держать под надзором указанных лиц и регулярно проводить профилактическую работу с учетом их психологических особенностей и характера.

2. Ограничение в использовании компьютерных технологий и информационно-телекоммуникационных сетей для лиц, осужденных за преступления в сфере компьютерной информации.

Большинство из преступлений в сфере компьютерной информации совершается с использованием сети «Интернет» и компьютерных технологий. Несомненно, возможность использования этих средств в повседневной деятельности, играет важную роль в жизни человека, но стоит учитывать, что в руках киберпреступников они становятся серьезным оружием, представляющим опасность для общества и государства.

Ограничение в их использовании на определённый период времени (в зависимости от личности киберпреступника и общественной опасности совершенного им деяния) является частью индивидуальной профилактической работы. Лишить злоумышленника оружия – один из важных элементов его исправления.

Вместе с тем появляется серьезный вопрос: «Как проконтролировать исполнение осужденным обязательства?». На наш взгляд, в специальном контроле нет необходимости. Если по каким-то причинам (по заявлению третьего лица) вскроется факт использования лицом информационно-телекоммуникационных технологий, то в этом случае условное наказание будет заменено реальным.

Подводя общий итог, следует отметить, что в число специально-криминологических мер предупреждения преступлений в сфере компьютерной информации стоит отнести меры общей профилактики, связанные с развитием международно-правового сотрудничества,

необходимостью разъяснения ВС РФ норм УК РФ, предусматривающих ответственность за преступления в сфере компьютерной информации, введением уголовной ответственности за создание, использование и продажу, систем удаленного использования чужих электронных устройств, внесением защитного программного обеспечения в список приложений, обязательных для установки в электронные устройства, продаваемые на территории Российской Федерации, а также блокированием сотовой связи на территории учреждений, исполняющих уголовные наказания в виде лишения свободы, и мест содержания под стражей . Индивидуальные меры профилактики должны включать профилактический надзор за киберпреступниками и введение ограничений на использование компьютерных технологий. Важно отметить, что перечень профилактический мер является открытым, в связи чем в будущем его необходимо дополнять и иными мероприятиями.

ЗАКЛЮЧЕНИЕ

В результате проведенного исследования поставленные цели и задачи были достигнуты в полном объеме.

С учетом всех имеющихся доктринальных и нормативных позиций удалось вывести собственное понятие преступности в сфере высоких технологий, под которым понимается исторически изменчивое, социальное и уголовно-правовое негативное явление, представляющее собой совокупность противоправных, общественно опасных посягательств, совершаемых с использованием наиболее новых и прогрессивных технологий современности в сфере экономики, общественной безопасности, здоровья населения, нравственности и компьютерной информации, а также лиц их совершающих, имеющее транснациональный и трансграничный характер.

Проанализировав состояние, структуру и динамику преступности в сфере высоких технологий мы пришли к выводу, что на сегодняшний день состояние данного вида преступности характеризуется большим количеством зарегистрированных преступлений, совершенных с использованием информационно-телекоммуникационных технологий. Их ежегодный прирост составляет более 50%, что говорит о высоких темпах распространения. В структуре преступности в сфере высоких технологий самыми популярными являются общественно-опасные деяния в сфере экономики, а наиболее предпочтительными средствами и орудиями совершения подобных преступлений является сеть «Интернет» и инструменты мобильной связи.

Определив характерные признаки личности, совершающей преступления в сфере высоких технологий было установлено, что в роли киберпреступников чаще всего выступают лица мужского пола среднего возраста (25-49 лет), имеющие высшее или среднее профессиональное образование. Они официально не работают, получают доход за счет преступной деятельности. Среди самых распространенных мотивов этих лиц выступает корысть, насилие, желание самоутвердиться, желание

дезорганизовать деятельность государственных органов и иных организаций, а также сексуальная озабоченность.

Среди основных причин преступности в сфере высоких технологий нами было выделено три основные группы: общесоциальные, социально-психологические и личностные. К общесоциальным причинам в политической сфере отнесены низкий контроль государства за средствами массовой информации и заинтересованность ведущих стран мира в использовании кибероружия. Причины экономической сферы обусловлены нестабильностью экономической обстановки в стране. Причины социальной сферы связаны с высоким уровнем компьютеризации населения. Правовыми причинами являются несовершенство уголовного законодательства и судебной практики. Среди иных причин преступности в сфере высоких технологий следует выделить высокую латентность этих преступлений, недостаточную эффективность деятельности подразделений правоохранительных органов и слабую защищенность финансовых сервисов. К числу социально-психологических причин отнесены проблемы взаимоотношения киберпреступников в семье, а также отсутствие необходимого контроля со стороны родителей и близких родственников. Помимо этого, имеется ряд проблем в школе, связанных с недостаточным воспитательным воздействием преподавателей на ученический коллектив. При проведении досуга киберпреступник подвергается негативному влиянию со стороны правонарушителей, с которыми он общается в виртуальном пространстве. Под этим давлением изменяется система ценностей и принципов лица. Причины личностного уровня раскрываются в механизме индивидуального преступного поведения. Киберпреступник всегда тщательно планирует свою противоправную деятельность, осторожно подбирает жертву преступления, высоко оценивает свои силы и возможности, при совершении преступления не испытывает чувства раскаяния и ответственности.

Установив причины, влияющие на преступность в сфере высоких технологий, нами были предложены общие и специальные меры предупреждения преступности в сфере высоких технологий.

К общим мерам предупреждения мы отнесли защиту конституционного строя, сохранение гражданского мира, политической и социальной стабильности в обществе, формирование условий для экономического роста и улучшения качества жизни населения, активизацию фундаментальных и прикладных научных исследований в области высоких технологий, развитие идеи недопустимости аморального поведения как в реальной, так и в виртуальной средах. Среди виктимологических мер предупреждения преступности в сфере высоких технологий были выделены мероприятия по активизации профилактической деятельности средств массовой информации, правовое просвещение и информирование молодежи, увеличение сроков переводов денежных средств через банки, а также внедрение новых способов идентификации клиентов банка.

Специальные меры предупреждения преступности в сфере высоких технологий были разделены на меры общей и индивидуальной профилактики. К мерам общей профилактики мы отнесли мероприятия, связанные с развитием международно-правового сотрудничества, необходимостью вынесения разъяснений норм главы 28 УК РФ, введением уголовной ответственности за оборот систем удаленного использования электронных устройств, предустановку защитного программного обеспечения в электронные устройства, продаваемые на территории Российской Федерации, а также блокирование сотовой связи на территории учреждений, исполняющих уголовные наказания в виде лишения свободы, и мест содержания под стражей. Индивидуальные меры профилактики преступности в сфере высоких технологий могут включать профилактический надзор за киберпреступниками и введение для них ограничений на использование компьютерных и информационно-телекоммуникационных технологий.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

Нормативно-правовые акты и иные официальные документы

1. Федеральный закон от 09.03.2021 № 44-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации в части прекращения оказания услуг связи на территории следственных изоляторов и учреждений, исполняющих уголовные наказания в виде лишения свободы" // Официальный интернет-портал правовой информации. URL: http://publication.pravo.gov.ru/Document/View/0001202103090043?index=0&rangeSize=1 (дата обращения: 23.03.2021).

2. Распоряжение Правительства Российской Федерации от 31.12.2020 № 3704-р // Официальный интернет портал правовой информации. URL: http://publication.pravo.gov.ru/Document/View/0001202101060012?index=2&rangeSize=1 (дата обращения: 25.03.2021).

3. Апелляционное постановление Московского городского суда № 10-11502/2013 от 25 ноября 2013 г. по делу № 1-9/13 // СПС «Право.ru». URL: http://docs.pravo.ru/document/view/69641175/81049299/ (дата обращения: 25.03.2021).

4. Приговор Октябрьского районного суда г. Уфы (Республики Башкортостана) № 1-243/2020 от 29 июля 2020 г. по делу № 1-243/2020 // Судебные и нормативные акты РФ. URL: https://sudact.ru/regular/doc/Nr1KqpqIfTLr/ (дата обращения: 23.01.2021).

5. Проект Концепции стратегии кибербезопасности Российской Федерации // Совет Федерации Федерального Собрания Российской Федерации. URL: http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf (дата обращения: 05.03.2021).

Монографии, учебники, учебные пособия

6. Козаев Н. Ш. Современные проблемы уголовного права, обусловленные научно-техническим прогрессом: Автореф. дис. … док. юрид. наук: 12.00.08. - Краснодар. 2016. С.430.

7. Компьютерные преступления: Способы совершения и раскрытия / под. ред. Вехова В. Б., Смагоринского Б. П. - М. : Право и Закон, 1996. С. 182.

8. Криминология (Общая часть): учебное пособие. / под. ред. Л. М. Прозументов, А.В. Шеслер. - Томск. 2017. С. 284.

9. Криминология: учебник и практикум для академического бакалавриата. / под. ред. Афанасьева О. Р., Гончарова М. В., Шиян В. И. М.: Юрайт. 2018. С. 360.

10. Криминология: учебник и практикум для бакалавриата и специалитета / под. ред. Козаченко И. Я., Корсаков К. В. М.: Юрайт. 2019. С. 277.

11. Лопатина Т. М. Криминологические и уголовно-правовые основы противодействия компьютерной преступности: дис. ... док. юрид. наук. - М. 2007. С. 418.

Научные публикации и статьи в иных периодических изданиях

12. Агарагимова И. Ф. Личность преступника в сфере высоких технологий: сборник научных статей студентов юридического факультета. // Проблемы совершенствования законодательства. 2019. №81/19. С. 83-86.

13. Атнашев В. Р., Яхъеева С. Н. Международное сотрудничество в борьбе с киберпреступностью и кибертерроризмом // Евразийская интеграция: экономика, право, политика. 2019. № 3. С. 37-42.

14. Евдокимов К. Н. Основные причины компьютерной преступности в современной России // The Journal of Siberian and Far Eastern Studies. 2014. №8. С.69-70.

15. Кабайкина О. В., Сущенко О. А. Трансформация роли женщины в современном обществе: в семье и на работе. // Вестник Московского университета. Серия 18. Социология и политология. 2017; Т.23. №3. С. 140-155.

16. Комаров А. А. О критериях общественной опасности, преступлений в сфере высоких технологий // Актуальные вопросы права, экономики и управления. 2017. С. 243-245.

17. Косенков А. Н., Черный Г. А. Общая характеристика психологии киберпреступника. // Всероссийский криминологический журнал. 2012. №3. С. 92.

18. Кушниренко С. П. Методика расследования преступлений в сфере высоких технологий // Конспект лекций, СПб юрид. ин-т Генеральной прокуратуры РФ. СПб. 2007. С. 4-18.

19. Лопатина Т. М. Проблемы формирования уголовно-правового способа борьбы с компьютерным мошенничеством // Библиотека криминалиста. 2013. № 5. С. 34 - 41.

20. Некрасова Н. А., Некрасов С.И. Философия науки и техники: Тематический словарь справочник. Учебное пособие. М.: МИИТ, 2009. С. 392.

21. Никеров Д. М., Хохлова О. М. Преступления в сфере высоких технологий в современной России // Вестник Восточно-Сибирского института МВД России. 2019. №2. С. 91.

22. Ситников Е.С. Закон об анонимайзерах: ответственность за посещение запрещенных сайтов в России. // NOVAUM.RU. 2018. №16. С. 437.

23. Чирков Д. К., Саркисян А. Ж. Преступность в сфере высоких технологий: тенденции и перспективы // Вопросы безопасности. 2013. № 2. С. 160 - 181.

24. Шалагин А. Е. Транснациональная преступность: понятие, признаки, меры противодействия // Вестник экономики, права и социологии. 2016. №3. С. 138-141.

25. Шевко Н.Р. Особенности раскрытия и расследования киберпреступлений: проблемы и пути их решения // Ученые записки Казанского юридического института МВД России. 2016 Т. 1. № 1. 2016. С. 13-16.

26. Назайкин А. Медиапланирование на телевидении // Бизнес-Ключ. 2007. № 1. URL: https://www.bkworld.ru/archive/y2007/n01-2007/n01-2007_182.html (дата обращения: 20.03.2021).

27. Рынок интернет-мошенничества в России // Исследования BrandMonitor. URL: https://media.brandmonitor.ru/rynok-internet-moshennichestva-v-rossii (дата обращения: 10.12.2020).

28. Юрьева В.Г. Психология преступного поведения и ее зависимость от акцентуации характера преступника // Вестник Таганрогского института имени А.П. Чехова. 2016. №1. URL: https://cyberleninka.ru/article/n/psihologiya-prestupnogo-povedeniya-i-ee-zavisimost-ot-aktsentuatsii-haraktera-prestupnika (дата обращения: 10.12.2020).

29. John Suler. The Psychology of Cyberspace // Department of Psychology Science and Technology Center Rider University. URL: http://users.rider.edu/~suler/psycyber/psycyber.html (дата обращения: 25.02.2021).

Интернет-ресурсы

30. Anonymous вывели из строя сайт Интерпола в ответ на аресты // Lenta. URL: https://lenta.ru/news/2012/02/29/anony (дата обращения: 11.12.2020).

31. Берг Е. Городская легенда. Что стоит за игрой «Синий кит» и всплеском интереса к «суицидальным пабликам? // Meduza. 2017. URL: https://meduza.io/feature/2017/02/17/gorodskaya-legenda-chto-stoit-za-igroy-

siniy-kit-i-vspleskom-interesa-k-suitsidalnym-pablikam (дата обращения: 15.12.2020).

32. Буркина В. Что такое хорошо? // Щит и меч. 2020. №48. URL: https://xn--b1aew.xn--p1ai/upload/site1/document_journal/Schit_i_mech__48_2020_skleyka.pdf (дата обращения: 01.03.2021).

33. Делюгин Е. Про сравнения с «Яндексом», нужды людей и захват рынка ассистентов: рассказывает конструктор техники от «Сбера» // VC.RU. URL: https://vc.ru/story/160830-pro-sravneniya-s-yandeksom-nuzhdy-lyudey-i-zahvat-rynka-assistentov-rasskazyvaet-konstruktor-tehniki-ot-sbera#security (дата обращения: 13.03.2021).

34. Заседание коллегии ФСБ России // Официальный сайт Президента Российской Федерации. URL: http://kremlin.ru/events/president/news/65068 (дата обращения: 21.04.2021).

35. Информация о деятельности Московского института новых информационных технологий ФСБ России // Официальный сайт Московского института новых информационных технологий ФСБ России. URL: http://minit.fsb.ru/minit/information.htm (дата обращения: 21.03.2021).

36. Кошкина Ю. Голосовой помощник Сбербанка может подсказывать мошенникам // Дайджест вкладчика. 2019. №110/948. URL: https://www.zvi2015.ru/article/1087 (дата обращения: 13.03.2021).

37. На фоне пандемии COVID-19 выросла активность телефонных мошенников и киберпреступников в Интернете // Официальный сайт Центрального банка Российской Федерации. URL: http://www.cbr.ru/press/event/?id=8238#highlight=%D0%BC%D0%BE%D1%88%D0%B5%D0%BD%D0%BD%D0%B8%D0%BA%D0%BE%D0%B2 (дата обращения: 01.03.2021).

38. Предотвращено распространение вредоносного программного обеспечения для хищения денег с банковских счетов // Официальный сайт

Министерства Внутренних Дел Российской Федерации. URL: https://inlnk.ru/rJMml (дата обращения: 25.03.2021).

39. Рейтинги телевидения // Mediascope. URL: https://mediascope.net/data/ (дата обращения: 20.03.2021).

40. Салют, Сбер! Переведи деньги // Официальный сайт ПАО «Сбербанк». URL: https://www.sberbank.ru/ru/person/promo/perevody-salut (дата обращения: 13.03.2021).

41. Сошников А., Рейтер С. Москит, Надежда, Наутилус: хакеры раскрыли суть проектов тайного подрядчика ФСБ // BBC News. URL: https://www.bbc.com/russian/features-49050982?fbclid=IwAR39d-JCwHnEQg7mHXFwwqChe7bwxu1bhuyIzgoHA16yqxwMbgINDbxk-38 (дата обращения: 07.03.2021).

42. Средства резервного фонда Правительства помогли частично покрыть дефицит школ и детсадов в Санкт-Петербурге // Счетная палата Российской Федерации. URL: https://ach.gov.ru/checks/zhitelyam-novykh-domov-v-sankt-peterburge-ne-khvataet-mest-v-detskikh-sadakh-i-shkolakh (дата обращения: 01.05.2021).

43. Устав ПАО «Нефтяной компании «Роснефть». // Официальный сайт ПАО «Роснефть». URL: https://www.rosneft.ru/upload/site1/document_file/rosneft_charter2.pdf (дата обращения: 10.12.2020).

44. Факультет информационной безопасности // Федеральная служба безопасности Российской Федерации. URL: http://academy.fsb.ru/i_faculty_ib.html (дата обращения: 21.03.2021).

45. Факультет подготовки специалистов в области информационной безопасности // Московский Университет МВД России имени В.Я. Кикотя. URL: https://inlnk.ru/W403P (дата обращения: 21.03.2021).

46. Хакеры из Anonymous атаковали сайт Ватикана // Lenta. URL: https://lenta.ru/news/2012/03/07/vatican/ (дата обращения: 11.12.2020).

47. Broad W. J., Markof J., Sanger D. E. Israeli Test on Worm Called Crucial in Iran Nuclear Delay // The New York Times. 2011. URL: https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html (дата обращения: 22.02.2021).

48. Chris Mills Judge Confirms Carnegie Mellon Hacked Tor and Provided Info to FBI // Gizmodo. URL: https://gizmodo.com/judge-confirms-carnegie-mellon-hacked-tor-and-provided-1761191933 (дата обращения: 07.03.2021).

49. Kaspersky Who Calls // Лаборатория Касперского. URL: https://www.kaspersky.ru/caller-id (дата обращения: 25.03.2021).

50. Peter Krapp. Terror and Play, or What was Hacktivism? // Grey Room. MIT Press. 2005. URL: https://www.researchgate.net/publication/238425073_Terror_and_Play_Or_What_Was_Hacktivism (дата обращения: 15.12.2020).

Эмпирический материал

51. Сводные статистические сведения о состоянии судимости в России за 2015 год. М. 2016.

52. Сводные статистические сведения о состоянии судимости в России за 2016 год. М. 2017.

53. Сводные статистические сведения о состоянии судимости в России за 2017 год. М. 2018.

54. Сводные статистические сведения о состоянии судимости в России за 2018 год. М. 2019.

55. Сводные статистические сведения о состоянии судимости в России за 2019 год. М. 2020.

56. Состояние преступности в России за январь-декабрь 2016 года. М. 2017.

57. Состояние преступности в России за январь-декабрь 2017 года. М. 2018.

58. Состояние преступности в России за январь-декабрь 2018 года. М. 2019.

59. Состояние преступности в России за январь-декабрь 2019 года. М. 2020.

60. Состояние преступности в России за январь-декабрь 2020 года. М. 2021.

61. Developer Survey Results 2019 // Stack Overflow Limited. URL: https://insights.stackoverflow.com/survey/2019 (дата обращения: 09.02.2021).

62. Global Wealth Report 2015 // Credit Suisse Group. URL: https://www.credit-suisse.com/media/assets/corporate/docs/about-us/research/publications/global-wealth-report-2020-en.pdf (дата обращения: 09.02.2021).

63. Simon Kemp. Digital 2021: Global overview report // DataReportal. URL: https://datareportal.com/reports/digital-2021-global-overview-report (дата обращения: 09.02.2021).