УДК 343.34:004
DOI: 10.26140/bgz3-2020-0903-0089

КИБЕРПРЕСТУПЛЕНИЯ И ПРЕСТУПЛЕНИЯ ПО ТЕЛЕФОНУ

SPIN-код: 1456-8470
Author ID: 968312
Гончарова Светлана Викторовна, подполковник полиции, старший преподаватель кафедры общеправовых дисциплин
SPIN-код: 9298-5870
Author ID: 884581
Полунина Елена Николаевна, капитан полиции, заместитель начальника кафедры общеправовых дисциплин
Ростовский юридический институт Министерства внутренних дел России, филиал в Волгодонске (347360, Россия, Волгодонск, улица Степная, 40, e-mail: moiseewa83@list.ru)

Аннотация. Количество киберпреступлений, особенно в сфере экономики, в последние несколько лет заметно выросло, как и количество мошеннических схем, которые осуществляются через телефоны и смартфоны. Данные правонарушения преследуются по уголовному законодательству. По статистике, за последние несколько лет эти преступления нанесли ущерба на значительные суммы денег. Данный факт позволяет сделать вывод об серьезной угрозе, которая идет сразу к нескольким сферам жизни общества, так как затрагивает и личные права граждан, и экономику целой страны. Однако, усилия правоохранительных органов не дают заметного результата в борьбе с новыми видами преступлений. Качественно проведенная проверка по сообщению о преступлении позволяет выявить основания для возбуждения уголовного дела. Своевременно возбужденное уголовное дело дает возможность найти следы преступления. Не смотря на вышесказанное, киберпреступлениям свойственны особые признаки и свойства, благодаря которым их очень трудно расследовать. Правоохранительный органы относят данные виды преступлений к наиболее редко раскрываемым. Данная статья посвящена проблемам совершенствования норм уголовно-процессуального законодательства, касающихся проведения проверки по сообщениям о киберпреступлениях. Рассматривается актуальность киберпреступлений, их виды и возможные способы их совершения, особенности киберпреступлений. Предлагаются соответствующие меры профилактического характера. Проводится анализ количества преступлений по РФ в данной области, а также тенденция роста и индексации количества правонарушений.

Ключевые слова: уголовный процесс, уголовное право, следственные действия, киберпреступность, проверка сообщений о преступлении, финансовые преступления, financial crimes, фишинг, кибероружие, кибертерроризм, фарминг.

CYBER CRIMES AND CRIMES BY PHONE

Goncharova Svetlana Viktorovna, police lieutenant colonel, Senior Lecturer, Department of General Law
Polunina Elena Nikolaevna, captain of the police, Deputy Head of the Department of General Legal Disciplines
Rostov Law Institute of the Ministry of Internal Affairs of Russia, Volgodonsk branch (347360, Russia, Volgodonsk, 40 Stepnaya street, e-mail: moiseewa83@list.ru)

Abstract. The number of cybercrimes, especially in the economic sphere, has increased markedly in the past few years, as has the number of fraudulent schemes that are carried out through phones and smartphones. These offences are prosecuted under criminal law. According to statistics, over the past few years, these crimes have caused damage to significant amounts of money. This fact allows us to draw a conclusion about a serious threat that goes to several spheres of society at once, as it affects both the personal rights of citizens and the economy of the whole country. However, the efforts of law enforcement agencies do not give a noticeable result in the fight against new types of crimes. A high-quality check on the report of a crime allows you to identify the grounds for initiating a criminal case. A timely criminal case makes it possible to find traces of a crime. Despite the above, cybercrimes have special features and properties that make them very difficult to investigate. Law enforcement agencies consider these types of crimes to be the most rarely solved. This article is devoted to the problems of improving the norms of criminal procedure legislation concerning verification of reports of cybercrime. The article considers the relevance of cybercrimes, their types and possible ways of their Commission, and the specifics of cybercrimes. Appropriate preventive measures are proposed. The analysis of the number of crimes in the Russian Federation in this area, as well as the growth trend and indexing of the number of offenses.

Keywords: crimil trial, crimal law, investigative actions, cybercrime, verification of a crime report, financial crimes, phishing, ceberweapons, farming.

ВВЕДЕНИЕ

Постановка проблемы в общем виде и ее связь с важными научными и практическими задачами.

В современном мире быстрое развитие получили информационные и цифровые технологии, которые поменяли структуру жизни общества, в том числе оказали влияние на финансовое и информационное поле. Прогрессирование киберугроз влечет за собой необходимость установления и обеспечения информационной безопасности на государственном уровне. Согласно мировым данным, а также непосредственной статистике в РФ, граждане имеют очень низкий уровень защищенности в сети Интернет. Проявляется данная уязвимость в обширном поле – от технических брешей, до уязвимости программ, обеспечивающих проведение операций с деньгами. В свою очередь, это вызвало появление злоумышленников, действия которых направились на данные ресурсы. Развитие информационной сети – Интернет, лишь способствовало появлению новых способов совершения преступлений, новых субъектов преступлений, а также целям и средствам их достижения. Современный уголовный кодекс РФ не содержит определения термина «киберпреступление». В актуальной юридической литературе под данным термином понимают «преступления в сфере компьютерной информации» или «информационные преступления». Первым из этих терминов и пользуется УК РФ, который выделяет преступления в сети Интернет в отдельную главу 28 «Преступления в сфере компьютерной информации».

Преступления, которые находятся под юрисдикцией УК РФ, а также совершаются в сфере компьютерных преступлений попадают под следующий перечень статей,

по которым задерживаются правонарушители: Ст. 110 УК РФ [1]. Доведение до самоубийства. Ст. 146 УК РФ. Нарушение авторских и смежных прав. Ст. 159 УК РФ. Мошенничество. Ст. 163 УК РФ. Вымогательство. Ст. 187 УК РФ. Неправомерное оборот средств платежей. Ст. 228 УК РФ. Незаконное приобретение, хранение… наркотиков. Ст. 242 УК РФ Незаконные изготовления и оборот порнографических материалов или предметов. Ст. 272 УК РФ. Неправомерный доступ к компьютерной информации. Ст. 273 УК РФ. Создание, использование и распространение вредоносных программ для ЭВМ. Ст. 274 УК РФ. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации.

Данная тенденция показывает то, что большинство преступлений, которые имеют место в реальной жизни совершаются и в сети интернет. Более того, совершение правонарушений сети делает их более сложными для обнаружения и проведения расследования. По состоянию на данный момент преступникам уже не требуется установление личного контакта с предполагаемыми потерпевшими для осуществления своих замыслов, злоумышленники теперь могут стать опасностью не только для физических лиц, но также для целых организаций, масштабных корпораций, а также целых государств.

.Таким образом, актуальность данной статьи заключается в широком распространении преступности в сети Интернет, необходимости определения киберпреступности, исследовании прогрессии темпах роста правонарушений в сети, низким уровнем информирования населения для профилактики преступлений, а также широким спектром риска стать потерпевшим от данного вида правонарушений, исследовании проблематики выявления преступления с помощью IT средств и преступлений в сфере IT технологий.

Как указывает в своей работе «Киберпреступления: понятие, содержания и меры противодействия» Павлюк А.В. и Бородкин Т.Н. В мае 2017 г. система распознавания вирусов компании Avast зафиксировала более 75000 заражений вирусом WanaCrypt0r 2.0 (aka WCry) в 99 странах мира [2].

МЕТОДОЛОГИЯ

Формирование целей статьи (постановка задания). Цель статьи – комплексное изучения киберпреступлений и преступлений, совершаемых по телефону, изучение с различных сторон понятия преступлений в информационной сфере, рассмотреть виды и особенности совершения таких правонарушений,

Анализ последних исследований и публикаций, в которых рассматривались аспекты этой проблемы и на которых обосновывается автор; выделение неразрешенных раньше частей общей проблемы.

В проблематике киберпреступлений многие авторы проводят свои исследования, благодаря чему юридическая литература предоставляет возможность к исследованию данного вопроса. Например, Бородкина Т.Н, в своей работе «Киберпреступление: понятие, содержание, и меры противодействия» поднимает актуальную проблему – вопрос понятия киберпреступления, разные трактовки этого понятия и способы, которые прикладываются для уменьшения ущерба и предотвращения подобных преступлений. Хорошо раскрывается тема классификации преступлений в сфере IT в работе Армасцева М.В. В его статье проводится анализ действующего законодательства, а также сравнение состава преступлений в реальном мире и киберпреступлений. Хорошо раскрываются разные методы теоретиков в определении понятия преступлений в IT сфере и их вреда обществу в рамках уголовного права.

Постановка задания. В данной статье проводится комплексное изучение проблем киберпреступлений, проблематике их обнаружений и раскрытий, их влиянию на граждан [3]. Помимо этого, затрагиваются преступления с использованием IT средств, а именно, преступления, совершаемые при помощи смартфонов.

РЕЗУЛЬТАТЫ

Изложение основного материала исследования с полным обоснованием полученных научных результатов. В начале исследования необходимо выделить определение термина «киберпреступление». Киберпреступление – это правонарушение, которое совершенно в электронной сфере, направленно на незаконное проникновение в работу компьютерных сетей, программ, устройств, с целью видоизменения данных, их изъятия или добавления ложной информации. В юридической литературе интересное и объемное определение термина «компьютерные преступления» дает Э.Л. Кочкина [4]. Она указывает, что данный термин представляет собой представляет собой совокупность преступлений, где в качестве непосредственного основного объекта преступного посягательства выступают охраняемые законом общественные отношения в сфере безопасного создания, хранения, обработки и передачи компьютерной информации, а предметом преступления являются компьютерная информация, средства защиты компьютерной информации, информационно-телекоммуникационные сети, средства хранения, обработки и передачи компьютерной информации. Такие преступления выполнены с помощи самой компьютерной системы, либо направленны непосредственно против нее. Данные правонарушения посягают на нарушение конфиденциальности данных, хранящихся в системе Интернет, а также базах данных юридических и физических лиц, с целью дальнейшего злоупотребление этими данными. При этом одним из обязательных признаков любого киберпреступления специалисты считают одновременное наличие двух объектов посягательства: как общественных отношений в сфере безопасности обращения компьютерной информации, так и связанных с ней общественных отношений, имеющих взаимосвязь с реальным миром.

Под преступлением в сфере обращения цифровой информации предлагается понимать предусмотренное уголовным законом виновно совершенное общественно опасное деяние, направленное на нарушение конфиденциальности, целостности, достоверности и доступности охраняемой законом цифровой информации [5].

Из определения можно сделать вывод, что киберпреступления разделяются на несколько видов и имеют ряд особенностей, которые помогают классифицировать данные деяния. К таким особенностям можно отнести: скрытный характер совершаемого преступления, а именно использование программ, которые дают анонимность и использование алгоритмов шифрования. Трансграничность – потерпевший и правонарушитель могут быть на любом расстоянии друг от друга, в том числе находится на территории разных государств. Нестандартность способов совершения – мелкие правонарушения совершаются по идентичным методам, однако крупные преступления совершаются практически каждый раз новыми способами, используются все новые системы декодирования и обхода систем защиты, а также путями запутывания следов. Следующей особенностью является автоматизированный режим совершения преступлений. Помимо этого, киберпреступления обладают наименьшим процентом раскрываемости из всех существующих видов преступления по статистике на каждый год. Сложность раскрытия обуславливается в том числе низким порогом обнаружения правонарушений. Создается это в том числе из-за непрофессионализма некоторых сотрудников, которые должны расследовать преступления, совершенные с использованием компьютерных сетей. Следует иметь ввиду следующее:

Во-первых, учитывая особенности компьютерной информации, необходимо обеспечить ее обязательное документирование в соответствии с установленным ГОСТом. Во-вторых, осмотр места происшествия, проводимый до возбуждения уголовного дела, является единственным процессуальным действием [6].

Киберспреступления охватывают достаточно широкую сферу общественных отношений. По цели данных преступлений, способу совершения и используемых программам, оборудованию можно составить классификацию данных деяний.

Первая группа составляет преступления против собственности, которые направлены на получения информации не санкционировано, а также незаконным путем, например, любое вмешательство в данные или незаконный доступ к информации [7].

Вторую группу составляют преступления, которые направлены на нарушение авторских, а, также, смешанных прав. Данный вид преступлений не во всех странах является уголовно преследуемым, однако в РФ это наказуемое деяние.

Третью группу составляют деяния, которые совершены с помощью технологий и программ. К таким относятся подлог, хищение, блокировка, подмена данных, любое другое получение выгоды незаконным путем.

Четвертую группу составляют наиболее тяжелые преступления, к которым относится кибертерроризм, а также эксплуатация виртуального пространства для совершения насильственных действий, деяний, которые посягают на общественную опасность.

На территории РФ совершается большое количество киберпреступлений, которые имеют динамику увеличения роста примерно 10% каждый год [8]. Меняется не только количество преступлений, но и объекты посягательства, иной качественный состав, а также размер причиняемого ущерба.

Если исследовать данные, которые предоставляет институт судебных экспертиз и криминалистики на период от апреля 2015 г. и до марта 2016 г. Злоумышленники успешно совершили кражи со счетов банковских компаний в РФ на денежную сумму в размере 348,6 млн рублей. Данные показатели превосходят показатели аналогичного периода за 2014-2015 год в пять раз. Российское информационное агентство ставит в известность о похищении 650 млн. р. с банковских карт физических и счетов юридических лиц в 2016 году. При этом большое количество случаев осуществляются методом социальной инженерии. В 2017 году показатель первого полугодия уже достигал 550 млн. руб., что составляет 85% от показателей за весь предыдущий год. По состоянию на 2018 год сумма ущерба от киберпреступлений в РФ составляет 400 млрд. рублей, по оценке Генпрокуратуры РФ [9]. За этот же год зарегистрировано 121247 преступлений, которые совершены с использованием телекоммуникационных технологий, а также в сфере компьютерной информации. Данный показатель на 44% больше, нежели показатели 2017 года. Однако, на начало 2018 года в мире с данным видом мошенничества столкнулись 31% организаций, по сравнению с 2016 показатель снизился на 1% (второе место среди экономических преступлений в мире), в Российской Федерации – 24 % (четвертое место среди экономических преступлений), в 2016 было 23%. Следует отметить, что данный показатель не является абсолютно точным в силу того, что: существует ограниченность при составлении выборки для проведения опроса с целью анализа данных; даже среди опрошенных организаций существует вероятность того, что респондент отвечал, что не пострадал от киберпреступлений, элементарно не подозревая об обратном.

Прием социальной инженерии хорошо описан в книге «Социальная инженерия и социальные хакеры» М.В. Кузнецова, И.В. Симдянова [10]. Согласно выдержкой из этой литературы – социальная инженерия представляет собой процесс манипулирования человеком или группой из нескольких физических лиц для осуществления цель взлома систем безопасности с последующими действиями вроде похищения важной информации и др. Такой вид преступлений является наиболее распространенным, так как не требует продвинутых навыков в сфере IT, денежных вложений в больших размерах и сложной системы запутывания следов.

В России получили широкое распространения следующие виды киберпреступлений:

1. Фишинг. Данный термин представляет собой извлечение информации путем вхождения в доверие граждан, которые далее становятся потерпевшими. В РФ хорошо развиты услуги интернет банков, приложения на Android и IOS, а также сайты в сети Интернет, через которые пользователи осуществляют денежные операции. Более серьезной версией обычного фишинга является целевой фишинг. Данный вид правонарушений направлен на массовую аудиторию. Типичный пример целевого фишинга – рассылка на почтовые адреса потерпевших сообщений, содержащих агитацию на переход на вредоносный сайт или скачивание программы с вредоносными троянами или иными вирусами.

2. Фарминг. Данный способ заключается в перенаправлении пользователей, которые совершают действия в сети Интернет на ложные IP адреса. Данный способ используется для имитации проверенных и надежных сайтов. Этот способ сложен в исполнении, но гораздо менее заметный, чем фишинг.

3. Кибероружие. В РФ, как и во многих странах мира активно применяется кибероружие для нарушения или уничтожения инфраструктуры. Такие вирусы могут быть несерьезными и направленными на спам или блокирование работы ПК обычных пользователей, а могут являться действительно серьезной угрозой для систем государственного значения или для банковских систем и других МФО. Создаются такие вредоносные ПО высокоуровневыми профессионалами, которые могут пользоваться продуктом в своих целях или продавать его другим злоумышленникам.

Киберпреступления зачастую предполагают перешедшую в электронную сферу версию обычных преступлений [11].

4. Кибер-порнография. К этой категории относятся ресурсы, которые дают пользователям возможность пользователям просматривать материалы эротического содержания с лицами, которые не достигли совершеннолетнего возраста.

5. Кибер-торговля наркотиками. Наркоторговля в сети является наиболее распространенным видом такой торговли в настоящий момент времени. При использовании такого метода преступники используют коды шифрования при отправлении на адреса покупателя писем, в которых содержится информация о местах, где происходит бартер наркотических веществ на деньги.

6. Кибертерроризм – совершение определенных террористических актов в пространстве сети Интернет. Примером данного вида преступлений можно привести распространение информации, которая содержит в себе описание и даты террористических актов, которые произойдут в ближайшем будущем. Интересы преступников лежат в энергетической сфере, финансовой, системе транспортных перевозок, военной и ядерной промышленности.

7. Теневые рынки. Так называемые черные рынки сейчас открыты для каждого желающего. Там продается разного рода товары, которые в том числе являются незаконными или содержат конфиденциальную информацию физических лиц, которая запрещена к распространению. Добытые путем кражи вещи, сканы и фотографии паспортов, все это продается и покупается злоумышленниками для совершения преступлений как в сети Интернет, так и за ее пределами.

Каждый день в мире происходит несколько тысяч кибератак [12]. Жертвами киберпреступников зачастую становятся подростки. Массовые доведения до самоубийства молодежи, иногда организуется преступниками для достижения неизвестных целей. Примером можно привести известную в прошлом группу «Синий кит», которая склонила большое количество молодежи к суициду, путем манипуляций и уговоров, а также воз-

действия на психику косвенными путями, вроде пропаганды сомнительных фильмов и литературы. Судебная практика уже имеет опыт судов над администраторами «групп смерти», и назначения им уголовных сроков, которые однозначно можно отнести к списку киберпреступлений.

Помимо этого, часто подобный вид преступности наблюдается именно среди подростков и людей от 20 до 25 лет. Связанно это с прогрессией мошеннических схем, в результате чего они становятся менее технически сложными и более доступными для применения, чем и пользуются молодые люди, преследуя цель легких денег.

Для борьбы со всеми видами компьютерных преступлений в первую очередь регламентируется уголовная ответственность за совершение таких деяний, которая предусмотрена УК РФ. Помимо того, органы МВД регулярно создают информационные пособия о том, как не стать жертвой таких преступлений, а также необходимым действиям, если избежать этого все же не удалось. Расследование таких преступлений зачастую осложнено тем, что разработка национальных систем борьбы с киберпреступлениями требует наличие специального образования и опыта, а также частное нахождение преступника и потерпевшего в разных государствах, что мешает следствию на критическом уровне. Помимо этого, проблему создает отсутствие развития нетрадиционных методов борьбы с киберпреступностью [13].

Следует отличать преступления, которые совершаются в сфере компьютерной информации от преступлений, которые совершаются с помощью ИТ. К такому виду преступлений чаще всего относят преступления, совершенные с помощью ПК, смартфонов, другой вычислительной техники. К преступлениям, которые совершаются по телефону чаще всего относится фишинг, который предполагает выведывание информации, или же склонение жертвы к переведению денежных средств на счета мошенников под разными предлогами. Такие преступления совершаются как путем звонка, так и с помощью SMS банкинга, другими письменными способами. Злоумышленники зачастую пользуются свойством банков «по умолчанию» включать в договор с клиентом банковской рассылки, в результате чего пользователи теряют бдительность, когда видят очередное письмо с номером банка. Потерпевшими таких преступников обычно становятся люди среднего и пожилого возраста, ведь именно они меньше всего ориентируются в современных преступных схемах в информационном поле системы Интернет, а также представляют собой наиболее уязвимые цели методов фишинга.

Данные преступления обычно преследуют цели хищения денежных средств, либо напрямую, либо путем использования различных электронных кошельков, которые нужны для получения денежного перевода и запутывания следов, путем пересылки денег между платежными счетами и дальнейшим выводом средств.

Способы совершения таких преступлений зачастую не отличаются друг от друга и имеют схожие сценарии. Преступник может отправить SMS сообщение, в котором говорится о несуществующем выигрыше в лотерею. Данный способ является хорошим примером социальной инженерии, где злоумышленник использует в качестве точки давления стремление человека к деньгам, доверчивость, а также входит в доверие иными способами, вроде имитации номера банка, например, Сбербанка (900).

Часто встречающимся видом преступлений является SMS рассылка с просьбой перечисления денежных средств под предлогом попадания в экстренную или непредвиденную ситуацию, что является целевым фишингом.

Распространенным способом преступлений, совершаемых по телефону является вымогательство, которое осуществляется с помощью шантажа и угроз распространения имеющимися у правонарушителя данных, порочащих честь и достоинство потерпевшего или членов его семьи.

Характерной чертой для таких преступлений, как и для киберпреступлений является анонимность преступника. Статистика показывает, что преступления в сети Интернет, а также преступления по телефону совершаются чаще всего одним лицом не как разовый акт, а как целая серия преступлений.

Проверка сообщений по данным правонарушениям происходит в 53% случаев по происшествии 10 дней со дня происшествия. В ходе опросов выяснено, что 95% сотрудников, работающих в сфере киберпреступности, имеют только юридическое образование, только оставшиеся 5% имеют дополнительное информационное [14].

При расследовании киберпреступлений правоохранительные органы сталкиваются с рядом проблем, которые сильно затрудняют ход расследования, а иногда делают его в целом невозможным. Главным препятствием на пути правосудия является возможность совершения анонимных действий в интернете. Как хорошо говорит в своей статье Захаров Д.Н. «Текущая ситуация такова, что лицо, совершающее противоправные действия, может находиться на территории Российской Федерации, но при этом использовать VPN-сервер…» При подобной схеме, ID пользователя уже находится в другой стране. Оплаты услуг таких серверов происходит за счет неперсонифицированных банковская карта, которая приобретается на теневых рынках и доставляется из другой части страны почтой России.

Большой проблемой для следователей является особенность проведения следственных действий, направленных на обыск и выемку технических средств. Для проведения экспертиз зачастую привлекается специалист, который не является экспертом по конкретному виду киберпреступлений. В результате неправильного взаимодействия теряется большая часть нужной информации и следов. Цифровые следы имеют высокую тенденцию трансформации и сложностью в отслеживании [15].

В последнее время в РФ все больше заботятся проблемой расследований киберпреступности. Для этого подготавливаются все более квалифицированные кадры. Для следователей, которые специализируются на раскрытии преступлений в сфере компьютерной информации организовали курс повышения квалификации, который получил название «Совершенствование деятельности подразделений предварительного следствия органов внутренних дел по расследованию преступлений в сфере компьютерной информации, совершаемых против собственности». Специалистов активно обучают тактическим методам, организационным моментам и уголовно, уголовно-процессуальным вопросам раскрытия такого вида преступлений.

*Результаты проделанной работы.*В статье рассмотрены актуальные на 2020 год виды киберспреступлений, как в мире, так и на территории РФ. С помощью исследованной информации можно сделать вывод, что преступниками, которые занимаются мелкими махинациями сфере киберпреступности являются молодые люди, в то время как крупные кибератаки и кибертеррористические акции относятся уже к разряду ОПГ. Потерпевшими от такого вида преступлений являются граждане любого возраста, однако больше всего подвержены именно люди в возрасте от 40 и выше лет, которые плохо знакомы с системой Интернет. Установлено, что раскрытию преступлений мешают факторы анонимности в сети и сложный процесс распутывание следов при работе следователей и криминалистов, а также низкий процент квалифицированных специалистов, работающих в сфере IT преступлений и киберпреступности.

ВЫВОДЫ

Выводы исследования. Исходя из проделанного в статье исследования можно сделать вывод, что киберпреступность набирает обороты с развитием инфор-

мационных и IT технологий. Расследовать такие преступления, несмотря на все предпринимаемые усилия остается очень сложно, ввиду целого ряда отягчающих факторов, среди которых есть и техническая сложность вопроса, и низкий уровень обращений граждан, которые стали потерпевшими в результате атаки киберпреступников. РФ активно взаимодействует с другими странами с целью поимки нарушителей и осуществлению правосудия, заимствует опыт зарубежных специалистов. Как указывает в своей работе «Особенности расследования киберпреступлений» Щерба В.В. и Захаров Д.Н. необходимо проведение дополнительных мероприятий по повышению уровня квалификации специалистов, работающих в данной сфере [16]. Помимо этого, необходимо учитывать международный опыт в данном вопросе для совершенствования собственной системы, а также предотвращению определенного процента преступлений в будущем.

Перспективы дальнейших изысканий в данном направлении.

Научные изыскания в данной теме просто необходимы, потому что на данный момент это одна из самых прогрессирующих тем в уголовном праве. Способы совершения киберпреступлений, их виды, способы их обнаружения и преследования будут дальше развиваться и прогрессировать наравне с развитием IT технологий, что делает необходимым их постоянный мониторинг, дополнение имеющейся информации и поднятие все новых проблем в сфере киберпреступности.

СПИСОК ЛИТЕРАТУРЫ:

1. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 06.07.2016). (Электронный ресурс) / Консультант-плюс. – 1999-2020. – Электрон. дан. – Режим доступа: http://base.consultant.ru.

2. Киберпреступления: понятие, содержание и меры противодействия. Бородкина Т.Н., Павлюк А.В. Социально-политические науки. 2018. № 1. С. 135-137.

3. К вопросу об уголовно-правовой классификации киберпреступлений. Арзамасцев М.В. Актуальные вопросы права и отраслевых наук. 2017. № 1 (3). С. 11-16.

4. Определение понятия «Киберпреступление». Отдельные виды киберпреступлений. Кочкина Э.Л. Сибирские уголовно-процессуальные и криминалистические чтения. 2017. № 3 (17). С. 162-169

5. Бегишев, И. Р. Понятие и виды преступлений в сфере обращения цифровой информации [Текст] / И. Р. Бегишев // Информационное право. – 2010. – № 2. – С. 18–21

6. Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества / А.Г. Волеводз. – М., 2002.

7. Третьяк, М. И. Проблема законодательной регламентации преступлений против собственности в сфере высоких технологий [Текст] / М. И. Третьяк // Законность. – 2016. – № 7. – С. 41–46.

8. Данные Генеральной прокуратуры Российской Федерации// Официальный интернет портал правовой статистики. (Электронный ресурс). URL: http://crimestat.ru/analytics.

9. Состояние преступности в России за ноябрь-январь 2017 г. - URL: https://мвд.рф/reports/item/ 11830347.

10. Социальная инженерия и социальные хакеры. Кузнецов Максим Валерьевич, Симдянов Игорь Вячеславович Жанр: Программирование, Информационные технологии ISBN: 5-94157-929-2 Год издания: 2007 Издательство: BHV.

11. Киберпреступность: криминологический, уголовно-правовой, уголовно-процессуальный и криминалистический анализ / науч. ред. И.Г. Смирнова; отв. ред. О.А. Егерева, Е.М. Якимова. – М., 2016.

12. Киберпреступления: основные проблемы расследования // Институт судебных экспертиз и криминалистики [Электронный ресурс]. 2015 Режим доступа: https://ceur.ru/library/articles/obshhie_stati/item196792.

13. Компьютерная криминалистика // Информационная безопасность. (Электронный ресурс). Режим доступа: http://http://www.itsec.ru.

14. Статистика кибератак в мире. (Электронный ресурс). Режим доступа: https://sicherheitstacho.eu/start/main.

15. Ефремова, М. А. Мошенничество с использованием электронной информации [Текст] / М. А. Ефремова // Информационное право. – 2013. – № 4. – С. 19–21.

16. Особенности расследования киберпреступлений. Захаров Д.Н., Щерба В.В Вопросы кибербезопасности №2(20) – 2017 стр. 72-76.

Статья поступила в редакцию 31.03.2020
Статья принята к публикации 27.08.2020