МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

Кафедра уголовного права и криминологии

ДИПЛОМНАЯ РАБОТА

на тему **«ПРЕСТУПЛЕНИЯ, СОВЕРШЕННЫЕ С ИСПОЛЬЗОВАНИЕМ КОМПЬЮТЕРНЫХ И ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ: ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ ИХ ПРЕДУПРЕЖДЕНИЯ ОРГАНАМИ ВНУТРЕННИХ ДЕЛ (РЕГИОНАЛЬНЫЙ АСПЕКТ)»**

Выполнил
Куланбаев Азамат Саматович
обучающийся по специальности
40.05.02 Правоохранительная деятельность
2017 года набора, 724 учебного взвода

Руководитель
доцент кафедры,
кандидат юридических наук, доцент
Бадамшин Ильфат Давлетнурович

К защите _____ рекомендуется
рекомендуется / не рекомендуется

Начальник кафедры _____ И.Р. Диваева
подпись

Дата защиты «___» _____ 2022 г. Оценка _____

ПЛАН

ВВЕДЕНИЕ

Неизмеримой особенностью современной действительности является повсеместное внедрение в жизнь практически каждого человека, вне зависимости от его гражданства, национальности, территориального нахождения, профессиональных, творческих и иных различных интересов, нового, более потенциально мощного инструмента средств массовой информации – глобальной информационно-телекоммуникационной сети «Интернет» во всем многообразии ее представления, использование которой в различных сферах жизнедеятельности государства позволяет утверждать о безоговорочной информатизации всего общества.

Сведения во всемирной сети распространяются молниеносно. И ничто им не является помехой – ни местоположение, ни время суток, ни цензура[1].

Более того, уже можно рассматривать выделение информационно-телекоммуникационных сетей в самостоятельную отрасль, о чем свидетельствует дальнейшее стремительное развитие веб-сайтов, мессенджеров, социальных сетей, составляющих конкуренцию традиционным средствам массовой информации.

Сфера «высоких технологий» дала нам множество возможностей и удобств: мы можем делиться новостями с друзьями, которые находятся за тысячи километров; можем отправить денежные средства своим близким людям для их нужд; можем совершать покупки, не выходя из дома; можем обмениваться личными тайнами, и многое другое. Телекоммуникационное пространство, в котором находится самая разная по своему наполнению и содержанию информация, безостановочно растет и данное явление не остановить. В данный период развития нашего общества, это пространство перестало быть чем-то теоретическим, оно превратилось во вполне ощутимую реальность.

---

[1] Шевко Н. Р. Интернет-технологии против терроризма // Противодействие терроризму и экстремизму в информационных системах: Сб. науч. ст. Всерос. конф. – М.: Московский университет МВД России имени В. Я. Кикотя, 2020. С. 80.

В частности, агенство We Are Social и сервис для SMM Hootsuite опубликовали ежегодное исследование состояния сферы диджитал (digital), согласно которому к началу 2022 года общее количество использующих «Интернет», составило 62,5% населения земного шара – 4,95 млрд. человек, увеличившись за 2021 год на 192 млн (4%). Количество пользователей социальных сетей выросло более чем на 10% и насчитывает 4,62 млрд – это 58,4% от общей численности населения всего мира[1].

Относительно Российской Федерации отметим, что если в 2010 году «Интернетом» пользовались 43,3 млн. человек, то уже к 2015 году – 78 млн. человек, в 2017 году – 87 млн. человек, в 2018 году – 92 млн. человек, в 2019 году – 95,9 млн. человек, в 2020 г. – 118 млн. человек (81% россиян), а уже в 2021 году, по состоянию на январь 2022 года – 129,8 млн. человек, что составляет 89% от общего количества населения России[2].

По данным исследования Brand Analytics «Социальные сети в России: цифры и тренды», проникновение «Интернета» в стране, в конце 2021 года составило 85%, активных авторов соцмедиа насчитывалось 66,4 млн. Более трети россиян, используя одну или несколько соцсетей, писали хотя бы один пост в месяц, а все вместе – 1,1 млрд. публичных сообщений (постов, репостов и комментариев). Наиболее популярными по размещению контента площадками стали: ВКонтакте, Instagram, Одноклассники, Twit-ter, YouTube, Facebook и TikTok[3].

Среднестатистический пользователь-россиянин проводит в «Интернете» каждый день более 7 часов, т.е. более 40% бодрствования. А во время существующий пандемии, в период частичной самоизоляции в учебе или

---

[1] Global Digital 2022: вышел ежегодный отчет об интернете и социальных сетях – главные цифры. Режим доступа URL: https://www.sostav.ru/publication/we-are-social-i-hootsuite-52472.html (дата обращения: 12.01.2022).

[2] Отчет «Digital 2022 Russian Federation» – Цифровые тенденции в России в 2022 году. Режим доступа URL: https://cpa.rip/stati/digital-2022-russian-federation/ (дата обращения: 12.01.2022).

[3] Социальные сети в России: цифры и тренды, осень 2021 // Блог Brand Analytics. Режим доступа URL: https://br-analytics.ru/blog/social-media-russia-2021/ (дата обращения: 12.01.2022).

работе в дистанционном формате некоторых организаций, эти цифры значительно увеличиваются[1].

Действующие платформы продолжают прирастать аудиторией, происходит активное появление новых участников. Причем данные сервисы далеко не всегда нацелены на позитивное объединение людей. Часто истинные цели создания и развития той или иной платформы тщательно скрываются.

К сожалению, совокупность применяемых и перспективных информационных технологий, все шире внедряемых в повседневную жизнь общества, является фактором, оказывающим значимое влияние как на позитивные, так и на негативные общественные характеристики.

Так, к настоящему моменту подтверждена прямая пропорциональная зависимость числа преступлений, совершаемых в киберпространстве, от количества пользователей сетей.

Таким образом, мир цифровых технологий за прошедшие несколько десятков лет стал неотъемлемой частью жизни большинства людей. Внедрение мировых информационных систем функционирует на основе глобальных компьютерных сетей, которые тесно связаны с совершенствованием информационных технологий. Особенно в быту, люди практически бесперебойно пользуются «дарами» цифрового развития, такими как, смартфоны, компьютеры, смарт-часы и т.д., при этом пользователи, не задумываясь, заполняют при регистрации свои личные данные, начиная от фамилии, имени и отчества и заканчивая номером своей дебетовой карты, включая все ее реквизиты.

Еще в начале XXI века, лидерами ведущих мировых держав было отмечено, что информационно-телекоммуникационные технологии являются наиболее существенными факторами, которые влияют на формирование современного общества. Однако развитие «высоких технологий» привело не только к высоким темпам развития индустриального общества, но и к

---

[1] Чуть меньше сна: сколько времени россияне сидят в интернете. Режим доступа URL: https://www.gazeta.ru/tech/2020/02/12/12956929/we_are_social.shtml (дата обращения: 12.01.2022).

появлению новых, ранее неизвестных источников опасности для него. Безопасность экономики и общества в целом, все больше зависят от стабильного функционирования глобальных сетей. Сбои в работе компьютерных сетей могут повлечь за собой серьезные последствия, как в жизни отдельного человека, в работе целых организаций и даже в функционировании безопасности и жизнеобеспечения отдельных государств в целом.

Данная угроза является «опасной» еще и благодаря тому, что уязвимостями компьютерных сетей, могут воспользоваться не только иные государства и террористические организации, но даже отдельные лица, с относительно невысоким уровнем знаний. Процесс «демократизации» в пользовании компьютерных и телекоммуникационных технологий, приводит к тому, что в настоящее время, даже отдельные лица, способны создать сбои в работе организаций и государственных структур, при этом, не обладая сверх мощными компьютерами и не затрачивая большие денежные средства. Вредоносная компьютерная программа или действия самих компьютерных злоумышленников в определенных обстоятельствах способны нанести ущерб крупнее, чем взрыв бомбы. При этом риск быть в дальнейшем обнаруженным, как правило, ниже, чем в «традиционных» видах преступлений.

Получая огромные преимущества от использования информационно-телекоммуникационных систем, наша страна, как и многие другие, крайне нуждается в стабильной, и бесперебойной их работе. Это заставляет Россию вырабатывать современные подходы к защите интересов личности, общества и государства в компьютерной среде. Актуально считать, что сфера «высоких технологий», обладая свойством воздействовать через виртуальное пространство на множество сфер жизни общества и государства, которые основываются на виртуальных данных, позволяет угрожать как частной собственности, так и государственной инфраструктуре.

Существенный вклад в изучение теоретических аспектов преступлений, совершаемых с использованием компьютерных и телекоммуникационных технологий, проблематике подходов по его нивелированию, механизмам и

мерам противодействия его распространению внесли такие отечественные ученные, как: Ю. М. Антонян, Ю. В. Гаврилин, С. В. Григоренко, Д. А. Ершова, М. Л. Есаян, Ю. В. Бельский, С. Я. Казанцев, А. А. Каспаров, А. Л. Осипенко, С. А. Солодовников, В. В. Меркурьев, В. А. Сапожникова, С. Н. Ткаченко, и др.

Нельзя упомянуть и зарубежный опыт, вклад в который внесли такие зарубежные ученые, например, М. Бреннер, С. Гудман, Ф. Вильямс, У. Зибер и многие другие, исследовавшие компьютерную преступность как явление, которое охватывает огромный спектр преступлений, совершаемых в мировом глобальном пространстве.

Объектом исследования являются общественные отношения, возникающие в рамках взаимодействия в информационно-телекоммуникационных сетях, а также основания уголовной ответственности за преступные деяния, совершаемые с применением глобальных сетей и компьютерных технологий.

Предметом исследования выступают сущность и содержание преступлений, совершаемых с использованием компьютерных и телекоммуникационных технологий и меры противодействия им.

Целью исследования является выявление содержания и форм реализации преступных деяний с применением компьютерных технологий и телекоммуникационных сетей, анализ теоретических и практических проблем их правового регулирования, а также разработка рекомендаций по совершенствованию мер их предупреждения.

Для достижения обозначенной цели в рамках данного исследования необходимо решить следующие задачи:

– рассмотреть содержание категории «преступления, связанных с использованием компьютерных технологий»;

– изучить общественную опасность преступных действий, совершаемых с использованием компьютерных и телекоммуникационных технологий;

– проанализировать состояние преступности в данной сфере в РФ и на международном уровне;

– разработать рекомендации по совершенствованию мер противодействия распространению преступлений, совершаемых с использованием компьютерных и телекоммуникационных технологий.

Структура исследования состоит из введения, двух глав, объединяющих в себе четыре параграфа, заключения и списка использованной литературы.

ГЛАВА 1. ОБЩАЯ ХАРАКТЕРИСТИКА И СОЦИАЛЬНАЯ ОБУСЛОВЛЕННОСТЬ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ КОМПЬЮТЕРНЫХ И ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

§1. Информационно-телекоммуникационные технологии и преступность: истоки и содержание

Впервые прототип «Интернета» появился в 1969 году, ею была сеть, которая могла передавать информацию адресату, даже при повреждении или уничтожении отдельных линий связи, именуемая ARPANET. Данный вид связи был создан Министерством обороны США. «Предок» Интернета обеспечивал параллельную автоматическую передачу информации по иным маршрутам в случае нестандартных ситуаций, при возможном возникновении которых, компьютер автоматически переключался с нарушенного маршрута на функционирующий.

В 1971 году ARPANET включал уже в себя отдельные университетские и правительственные сети компьютеров. Начальный набор услуг, предоставляемый пользователям, составлял лишь удаленную связь между пользователями, а именно обмен сообщениями. С ростом числа пользователей в APRANET, увеличивался и функционал. Так, в 1973 году к сети подключился первый пользователь из-за рубежа (Лондон).

Ввиду того, что число пользователей не отличалась большим количеством, все они, как правило, были знакомы друг с другом лично, и часто делились своей почтой для отправки той или иной информации не со своего компьютера. Таким образом, так называемый несанкционированный доступ и пользование чужой учетной записью, на тот период времени, не считался чем-то противоправным.

Первый громкий инцидент в деятельности связанный со взломом учетной записи был зафиксирован Клиффордом Столлом, в 1989 году. Тогда, неизвестное лицо взломало учетную запись одного из учеников,

предполагается, что путем подбора пароля. Столл стал первым, кто пытался привлечь внимание к уязвимостям APRANET.

В последующем, инцидентом, продемонстрировавшим плохую защищенность сети, стало появление «червя Морриса». Обучающийся американского университета, Роберт Моррис, написал программу, которая способна путем подбора пароля взламывать учетные записи пользователя, используя уязвимость сети. При этом программа саморазмножалась, и заражала другие компьютеры. Сам создатель «червя» пытался остановить этот процесс, однако понял, что вирус перестал быть контролируемым, и Моррис сообщил о содеянном директорату университета. Из-за инцидента, сеть APRANET была парализована на 10%, то есть это на тот момент – 70 000 человек подключенных сети, а сам ущерб от действий Морриса оценивается примерно в $ 96,5 млн.

Именно тогда появилась и первая команда специалистов по нейтрализации компьютерных угроз, которая в последующем, носила аббревиатуру «CERT». В дальнейшем, количество таких команд значительно увеличилось, и для координации их деятельности была создана общественная организация, именуемая как Форум Группы Реагирования на Инциденты и для Обеспечения Безопасности (F.I.R.S.T.).

1989 год ознаменовал для APRANET начало новой истории. В этом году Интернет стал носить всем уже знакомое нам имя. Тогда сеть уже не являлась правительственной, а число соединенных в единую сеть компьютеров превысило 100 тыс. Одновременно с этим, в Европейской лаборатории физики высоких энергий (Conseil Europeen pour la Recherche Nucleaire, CERN) Т. Бернерс-Ли предложил новые способы представления данных для использования гипермедиа системы, оно стало носить название World Wide Web. Эти методы значительно облегчали использование сетевого пространства, и это обеспечило мгновенный приток новых пользователей, не имеющих специальных познаний в области компьютерных технологий. Принято считать, что массовое использование Интернета началось в 1994 году, в связи с появлением программного обеспечения «Netscape Navigator», который

существенно облегчил процесс получения информации и обеспечил обработку различных видов данных, что само собой упростило освоение людьми компьютерных технологий.

Дальнейшее, беспрецедентное и лавинообразное развитие Интернета связано с ее коммерческим использованием и возможностью подключения к ней практически всех желающих. Одновременно это привело и к появлению новых проблем обеспечения безопасности передаваемых данных. Для нарушения бесперебойного функционирования сети требовалось больше действий и знаний, но и способы противодействия заметно усложнились. Ярким примером служит, широко распространившееся в 1994 году инструментальное средство для автоматизированного перехвата сетевых данных (sniffers), позволяющее легко получить доступ к именам и паролям других пользователей[1].

На сегодняшний день «глобальная мировая паутина» явно не стала более безопасной. Направления ее использования кардинально изменились. Возможности, предоставляемые обществу через информационно-телекоммуникационные сети, действительно огромны, но связанные с ними опасности также не менее значительны.

Появление доступа в Интернет в России датируется 1990 годом, когда Хельсинский университет зарегистрировал домен (.su), который означал доменную зону СССР в Интернете. А уже три года спустя был зарегистрирован российский домен (.ru).

В рамках существующих реалии, то есть на современном этапе развития Интернета, одной из основных присущих проблем, является та, что при работе в сети наблюдается полное отсутствие идентификаторов, и в данной связи, отсутствие информации о всех пользователях и их адресах в Интернете создает большие трудности в выявлении лиц, осуществляющих противоправные действия.

---

[1] Осипенко А. Л. Борьба с преступлениями в глобальных компьютерных сетях: Международный опыт: Монография. М.: Норма, 2018. С. 285-311.

Простота и анонимность в сети приводит к психологическому чувству безнаказанности и, следовательно, к возможности объединения лиц, осуществляющих противоправную деятельность, формированию преступных групп в сети, вовлечению в них различных организаций.

Значительное ослабление контроля над криптографией во многих странах привело к широкому использованию программного обеспечения среди обычных пользователей Интернета.

Доступ к компьютерной системе обычно приводит к использованию специальных технических или программных средств, которые позволяют отключить систему безопасности или получить доступ к ресурсным паролям.

Обычно, «доступ» подразумевает подключение к другой компьютерной системе через телекоммуникационные сети, и в этом случае способ связи может быть совершенно другим.

Статья 272 Уголовного Кодекса Российской Федерации (далее – УК РФ) устанавливает наказание за неправомерный доступ к охраняемой законом компьютерной информации, только если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы электронно-вычислительных машин (далее – ЭВМ), системы ЭВМ или их сети. Бытует мнение, что «сам по себе факт просмотра компьютерной информации, хранящейся на машинном носителе, состава анализируемого преступления не образует. Необходимо, по крайней мере, установить факт переноса указанной информации на другой машинный носитель»[1].

Однако в данной связи следует отметить, что в определенные моменты уже сам факт несанкционированного ознакомления виновного с данными постороннего лица может нанести ущерб. Таким образом, проблема привлечения лица к ответственности за непосредственное восприятие информации без копирования электронных носителей при незаконном доступе к системе чрезвычайно сложна из-за трудностей с доказательствами.

---

[1] Гаврилин Ю. В. Расследование неправомерного доступа к компьютерной информации. М., 2020. С. 106.

Так, например, В. В. Крылов отмечает, что «если придерживаться понимания термина копирования только как процесса изготовления копии документированной информации в виде физически осязаемого объекта, то все случаи, не связанные с копированием, но приводящие к ознакомлению с информацией независимо от того, какой режим использования информации установил ее собственник, не являются противоправными»[1].

С другой стороны, учитывая технологические особенности передачи информации в компьютерных сетях, добавление информации через монитор, даже если система не допускается на расстоянии, можно отнести к копированию такой информации.

Полученную неточность можно устранить, скорректировав текст ст. 272 УК РФ, включив в нее признак: «несанкционированное ознакомление лица с информацией …».

Исследование судебной практики показывает, что одним из наиболее выявляемых сетевых преступлений является использование похищенных сетевых реквизитов, которые обеспечивают доступ правонарушителя к Интернету. В таких случаях, преимущественно, уголовное дело возбуждалось по признакам преступления, предусмотренного ст. 272 УК РФ.

К сожалению, сложившийся опыт, кажется, не всегда оправдывает себя. Прежде всего, вызывает сомнения указание в качестве обстоятельства, допускающего вменение ст. 272 УК РФ, на происходящее в подобных ситуациях, модификацию учетно-статистической базы провайдера. В то же время, данные о незаконных сессиях доступа в Интернет лиц, указанных в базах данных провайдера, не могут рассматриваться как факты неправомерной модификации указанной учетно-статистической базы данных.

При квалификации преступления по ст. 272 УК РФ, в подобных случаях, в обязательном порядке должны учитываться обстоятельства способа получения неправомерно использованных реквизитов доступа. Данные реквизитов часто становятся известны злоумышленнику в результате

[1] Антонян Ю. М. Мотивация преступного поведения: монография. М.: Издательство: Юрлитинформ, 2018. С. 65.

беспечности их владельца, который самостоятельно способствует их получению третьими лицами.

Стоит иметь ввиду и те случаи, когда злоумышленник проникал в саму базу данных провайдера, и копировал оттуда реквизиты, содержащие пароли доступа к сети Интернет. В подобных ситуациях явно присутствует признаки состава преступления, предусмотренного ст. 272 УК РФ. При этом случаи копирования реквизитов, содержащих пароли доступа с баз данных провайдера, регистрируется гораздо чаще. И часто это сопровождается изменением самой базы данных для удаления зарегистрированных сеансов пользования злоумышленником, что увеличивает латентность преступного деяния.

Еще один яркий пример опасности и глобальности компьютерных преступлений – это взлом сайтов как отдельных лиц, так и правительственных сайтов.

Есть огромное количество фактов взлома, которые получили довольно широкий резонанс в прессе. К примеру, в 2016 году произошла атака на серверы Демократической партии США. Преступники подключились к серверу партии демократов для управления информацией и слежки за пользователями. После совершенных действий, хакеры устранили все улики. Выяснилось, что Хиллари Клинтон, являясь высокопоставленным политиком и кандидатом в президенты, отправляла и получала конфиденциальную информацию через личный почтовый ящик.

Или другой пример[1]. В 2000 году 15 летний подросток, из Майами, Джонатан Джеймс, в свое свободное время интересовался сайтом Министерства обороны США и случайно наткнулся на возможность обойти защиту сайта. Подростку удалось поместить на сервер вирус-шпион для захвата корреспонденции между сотрудниками Министерства. Это обеспечило свободный доступ к паролям и персональным данным сотрудников различных подразделений. Джонатан узнал код, который НАСА использовало для защиты системы жизнеобеспечения на Международной космической станции.

[1] Григоренко С. В., Ткаченко С. Н., Каспаров А. А. Преступления в сфере компьютерной информации. М., 2019. С. 101.

Нанесенный ущерб оценили в $ 1,7 млн. долларов, а подросток был приговорен к шести месяцам домашнего ареста.

Довольно часто несанкционированный доступ к телекоммуникационной системе осуществляется при подготовке к совершению сетевых преступлений. Например, нарушение системы Интернет-магазина часто направлено на полное или частичное прекращение работы магазина (недобросовестная конкуренция), изменение информации, размещенной на сайте Интернет-магазина (подготовка к совершению мошенничества), фальсифицированное предложение (кража денежных средств) и др.

Во многих случаях акты несанкционированного доступа крупных компаний к телекоммуникационным системам сопровождаются попытками раскрыть информацию, полученную незаконным путем, или попыткой потребовать крупные суммы денег с угрозой продолжения покушения на систему. В такой ситуации пострадавшие компании, как правило, стараются скрыть информацию о проникновении в их системы, так как это может серьезно повлиять на их репутацию.

Так, известны случаи выплаты хакерам крупных сумм. В частности, американская страховая корпорация (CNA) предложила хакерам выкуп в размере 40 миллионов долларов за возврат доступа к своим данным, который был заблокирован в связи с воздействием на него неизвестного вируса. По данным Bloomberg, злоумышленники первоначально потребовали $ 60 млн., однако после длительных переговоров согласились сократить сумму до $ 40 млн[1].

Кроме иностранных, компьютерных преступников, довольно большую активность возымели и российские хакеры. В 2001 году, пара преступников из России совершили попытки проникнуть в компьютерные системы нескольких зарубежных банков, таких как Western Union, PayPal и другие. Они сообщили банкам, что могут нанести значительный ущерб их системам, если не

---

[1] Хакеры выбили крупнейший в истории выкуп из корпорации, атакованной шифровальщиком. – URL: https://www.cnews.ru/news/top/2021-05-26_hakery_poluchili_rekordnyj (дата обращения: 03.03.2022).

предоставят выкуп. Во время одного из переговоров сотрудники ФБР смогли вычислить местоположение злоумышленников, и передали информацию о факте вымогательства в Интерпол. Если бы не совместные действия правоохранительных органов двух стран, то преступники нанесли бы колоссальный ущерб иностранным банкам, и остались бы безнаказанными. Сам факт того, что существует возможность получить огромную сумму денежных средств, без риска наказания подталкивает лиц, с устойчивым противоправным поведением искать способы для совершения аналогичных преступлений. Участившиеся случаи преступлений, совершаемых с использованием информационных и телекоммуникационных технологий, говорит о том, что огромное лиц, имеющих познания в сфере компьютерных технологий, уже вступили на преступный путь.

Так, говоря о росте числа компьютерных преступлений, нельзя упомянуть, что из-за большой популярности сети Интернет, увеличился рост числа преступлений, связанных с нарушением авторского права. Ассоциация производителей программного обеспечения для бизнеса (Business Software Alliance, BSA), в 2016 году выявила более 13 миллионов сайтов которые в той или иной степени были связаны с незаконным распространением защищенного авторским правом мультимедийные продукты, а ежегодные финансовые потери от «пиратства» участников ассоциации составили около 23 млрд. долларов США. По разным оценкам, оборот «пиратских продуктов» по ценам российского «черного рынка» составляет $ 10-50 млн. Ежегодные потери правообладателей составляют от 200 миллионов до 1 миллиарда долларов[1].

Огромный заработок на продаже «пиратского» программного обеспечения и слабая развитость правоприменительной системы в делах о привлечении к ответственности лиц, совершающих преступления в отношении авторских прав, стали основными причинами для формирования специализированных в этой сфере преступников. Как итог, на данный момент

---

[1] Ущерб от компьютерного пиратства: цифры и факты. – URL: http://adobereal.ru/index.php/pravovye-aspekty/ushcherb-ot-kompyuternogo-piratstva-tsifry-i-fakty (дата обращения: 03.03.2022).

93% всех программ, реализуемых в России, являются незаконными копиями, что сулит стране внешнеполитическими и внешнеэкономическими последствиями[1].

Стоит иметь в виду, что сам неправомерный доступ к чужим данным, как правило, является лишь инструментом для достижения более крупной цели, а именно для совершения таких преступлений, как нарушение личной неприкосновенности, нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сведений, незаконное приобретение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну (ст.ст. 137, 138, 183 УК РФ). Совершение указанных преступлений достигается посредством хранения информации в сетевых системах или электронного сбора данных. Проблема защиты прав человека на неприкосновенность частной жизни в условиях развития глобальных компьютерных сетей рассматривается как одно из самых трудноразрешимых правонарушений в развитых странах, из-за чего законом решается вопрос определения оптимального соотношения интересов личности и общества.

Европейские ученые-правоведы занимаются изучением нарушений конфиденциальности в глобальных компьютерных сетях путем мониторинга выносимых законодателем решений, а именно осуществляют обзор судебных дел в части, касающейся преступлений и правонарушений, связанных с информационными и телекоммуникационными технологиями и сбором информации о поведении людей в Интернете. На данный момент ученые относят к нарушению прав человека – мониторинг личных данных, разглашение данных с банковских карт, чтение электронной переписки и сбор сведений о поведении лица в Интернете.

Одно из таких противоправных деяний может проиллюстрировать следующий пример.

24 августа 2021 года из серверов компании Oriflame были украдены 1,5 миллиона паспортных данных россиян. Все данные были опубликованы в

[1] Пиратское ПО в России и мире. Нелицензионное ПО. – URL: https://www.tadviser.ru/index.php (дата обращения: 03.03.2022).

свободном доступе. Управляющий RTM Group, сообщил, что база данных из 1,5 млн. сканов паспортов на «черном рынке» будет оцениваться в более чем 100 тысяч долларов, так как с помощью данных сканов свободно можно оформить получение микрозайма или зарегистрировать сим-карту или кошельки электронных платежных систем. Электронные кошельки, регистрируемые с помощью паспортных данных, имеют большую степень «доверия» со стороны приложения, в отличие от обыкновенных.

Основное преимущество первых от вторых в том, что они намного реже блокируются за подозрительные действия и позволяют проводить более крупные транзакции[1].

Стоит упомянуть и еще один вид компьютерных преступлений, а именно компьютерный шпионаж. В расследовании и раскрытии данного вида преступлений существуют множество трудностей. Опасность этого явления в том, что в сетевых компьютерных системах сконцентрировано большое количество информации, которую легко получить с помощью современных технологий. И тенденция к росту в сети важной информации, неуклонно заставляет расти и факты совершаемых компьютерных шпионажей.

Например, в 2019 году был вынесен приговор двум сотрудникам банка, имеющим доступ к информации о счетах клиентов в Республике Саха. Они готовили кассовые заказы на основе информации, которая была у них на работе, а затем снимали деньги со счетов клиентов. Суд постановил, что логин и пароль для банковских систем, известный виновным, является коммерческой тайной Банка, о чем сотрудники были предупреждены, а также об ответственности за ее незаконное использование. Однако они использовали эту информацию в своих корыстных целях. Суд признал их виновными в совершении преступления, предусмотренного ч. 3 ст. 183 УК РФ, и приговорил их к трем и к четырем годам лишения свободы, соответственно[2].

---

[1] Григоренко С. В., Ткаченко С. Н., Каспаров А. А. Указ. соч. С. 109.

[2] Приговор Канашского районного суда (Чувашская Республика) № 1-29/2019 от 19 марта 2019 г. – URL: https://sudact.ru/regular/doc/Sz3pRC3muCgE/ (дата обращения: 05.03.2022).

На данном этапе развития экономики, многие страны крепко встали на путь рыночной экономики, что в совокупности с необходимостью обмениваться информацией на дальних расстояниях, заставило различные промышленные фирмы и организации делиться и хранить информацию в сетях Интернета. И это в свою очередь вызвало рост всех видов промышленного шпионажа, который участился на сегодняшний день и на территории России. В 2011 г. китайскими хакерами были взломаны компьютерные системы 5-ти транснациональных нефтегазовых компаний, откуда была скопирована информация об инвестиционных планах, планах по участию в торгах, заключению договоров, проведении разработок месторождений газа и нефти и другую информацию. Об этом сообщила компания McAfee (американская компания, разработчик антивирусного программного обеспечения) в своем отчете, однако названий взломанных компаний не раскрыли. Согласно отчету, источником атаки являлись сервера китайских провинций Пекина. Полученные данные были очень ценны, ввиду того, что разглашение этой информации конкурентам было способно сильно повлиять на решения различных нефтяных компаний[1].

Так же, в данной связи отметим, что немаловажными преступлениями, которые могут быть совершены с помощью компьютерных технологий и информационно-телекоммуникационных сетей, являются преступления, предусмотренные ст. 275 УК РФ «Государственная измена» и ст. 276 УК РФ «Шпионаж». Данные виды преступлений на данном этапе развития технологий сейчас легко осуществимы, и компьютерные технологий открыли для шпионажа и государственной измены огромные возможности.

Стоит иметь ввиду что, и профессиональные преступные организации активно участвуют в аналогичных преступлениях, ввиду огромных возможностей при получении крайне важной информации. Опыт зарубежных правоохранительных органов демонстрирует нам что организованные

---

[1] Жертвами китайских хакеров стали пять нефтяных гигантов. – URL: https://oilcapital.ru/news/markets/11-02-2011/zhertvami-kitayskih-hakerov-stali-pyat-neftyanyh-gigantov (дата обращения: 05.03.2022).

преступные организации активно пополняют сумму своих денежных средств за счет использования коммерческой тайны, как правило, получаемая путем взлома сайтов и серверов крупных организаций и фирм.

Так, 2018 году было нейтрализовано огромное количество Интернет-маршрутизаторов, взломанных российской хакерской группой «Fancy Bear». Преступная организация заразила своим вредоносным программным обеспечением около 500 тысяч Интернет-маршрутизаторов марок Linksys, MikroTik, NETGEAR и TP-Link. Данной операцией были сорваны планы киберперступников, которые с помощью зараженных устройств смогли бы получать информацию о логинах и паролях всех, кто подключался к Интернет-роутерам, а также имели бы возможность удаленно управлять электронной вычислительной машиной.

Далее отметим, что со становлением экономики Российской Федерации на путь компьютеризации, наша экономическая структура сделала еще один шаг в сторону развитых технологических государств[1]. Но одновременно с новыми технологиями пришли и новые опасности. Российская экономика легко адаптировалась к электронным средствам платежа, однако способы защиты платежных карт и находящихся в ней денежных средств развивались с некоторым опозданием их внедрению. Согласно характеристике состояния преступности[2], темп роста преступлений, совершенных с использованием информационных и телекоммуникационных преступлений в 2021 году заметно увеличился по сравнению с темпом роста преступности в 2020 году.

Наиболее часто регистрируемыми преступными деяниями в сфере компьютерных и телекоммуникационных технологий являются:

- мошенничество с использованием электронных средств платежа (ст. 159.3 УК РФ).

---

[1] Паспорт национального проекта «Национальная программа «Цифровая экономика Российской Федерации»» (утв. президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 04.06.2019 № 7). – URL: https://digital.gov.ru (дата обращения: 10.03.2022).

[2] Портал правовой статистики Генеральной Прокуратуры Российской Федерации. – URL: http://crimestat.ru/analytics (дата обращения: 10.03.2022).

Электронное средство платежа – средство или способ, позволяющие клиенту оператора по переводу денежных средств составлять, удостоверять и передавать распоряжения в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации, в том числе платежных карт, а также иных технических устройств[1]. Данный вид преступления получил резкий рост в числе зарегистрированный преступлений в 2019 году[2], и составил на тот момент 6 613 зарегистрированных фактов совершения преступления. Отметим, что преступление, предусмотренное ст. 159.3 УК РФ, является одной из самых сложных и тяжело расследуемых форм хищения, поэтому данное деяние отличается высокой степенью латентности;

- неправомерный доступ к компьютерной информации (ст. 272 УК РФ).

Данный вид преступлений подразумевает незаконное получение доступа к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации. В 2021 году было зарегистрировано 517 722 преступлений, связанных с хищениями с использованием информационных технологий, что всего на 1,44% больше, чем в 2020 г. (510 396 преступлений). Однако это почти вдвое превышает цифру 2019 года – 294 409 зарегистрированных преступлений. Большую тревогу, чем количество данных преступлений вызывает тот факт, что общая раскрываемость данной категории дел составляет в среднем 20% ежегодно;

- неправомерный оборот средств платежей (ст. 187 УК РФ).

Это изготовление, приобретение, хранение, транспортировка в целях использования или сбыта, а равно сбыт поддельных платежных карт, распоряжений о переводе денежных средств, документов или средств оплаты, а

---

[1] О национальной платежной системе: федер. закон Рос. Федерации от 27 июня 2011 г. № 161-ФЗ // Собр. законодательства Рос. Федерации. – 2011. – № 27, ст. 3872.

[2] Портал правовой статистики Генеральной Прокуратуры Российской Федерации. – URL: http://crimestat.ru/analytics (дата обращения: 10.03.2022).

также электронных средств, электронных носителей информации, технических устройств, компьютерных программ, предназначенных для неправомерного осуществления приема, выдачи, перевода, денежных средств. В данной связи наибольшую известность приобрел – биткоин (от английского слова bit – единица измерения количества информации, и coin – монета) – платежная система, которая использует одноименную единицу для учета операций. Под конец 2020 года курс биткоина вырос на 49%, до уровня $ 10 700.

Биткоин использует криптографические методы, для своей защиты, ввиду чего любой желающий может увидеть все его транзакции у любого из пользователей. Уже давно ожидалось, что интерес и спрос инвесторов может увеличить эти активы на новый ценовой уровень. Так и случилось.

Заинтересованность в криптовалюте, однако, проявили также и злоумышленники. Это связано с ее анонимной природой и той легкостью, с которой пользователи могут отправлять средства по всему миру. Так или иначе, главная цель любого криптовалютного преступления – обналичить деньги. Интерес преступников в данном случае ясно понятен. Отсутствие каких-либо данных о владельце, и удобство, которое помогает осуществлять движение биткоина в любую точку мира, крайне привлекательны для любого киберпреступника. В связи с этим, отмывание денег с помощью биткоина происходит крайне часто.

Однако, порой даже в самых идеальных преступных схемах, отмывание денег является самым важным звеном, которое часто происходит при помощи криптовалюты. А это может стать «ахиллесовой пятой», так как все действия в блокчейне можно отследить

Злоумышленникам затруднительно использовать серьезные биржевые ресурсы, вместо этого они используют удивительно небольшое количество одних и тех же услуг, связанных с отмыванием денег.

Часто преступники используют различные сетевые игры, в которых возможен ввод и вывод денежных средств, различные серверы со слабой организацией. Обычно это можно отследить путем наблюдения за тем, насколько популярен ввод и вывод денежных средств среди игроков или

сотрудников в игре или сервисе. Для некоторых сетевых игр действительная прибыль с покупки внутриигровых предметов крайне мала, и можно предположить, что такие сетевые игры и сервисы созданы для оказания услуг по обналичиванию.

Все денежные средства, добытые нелегальным путем, в основном размещались в 5 криптовалютных адресах. За несколько лет двое из данных адресов до сих пор используются в цепочке «отмывания» нелегальных денег. Речь идет о таких фирмах как Bitzlato и Garantex, Eggchange, Buy-bitcoin и Tetchange. Адреса этих 5 сервисов составили 55% от всех незаконных средств в 2020 году. Bitzlato и Garantex до сих пор отмечаются в цепочке «отмывания» нелегальных денег.

Так, например, в 2021 году, через Bitzlato было пройдено более 966 млн. долларов средств, которые обозначились как подозрительные операции. Эта операция составила более половину всех средств, которые прошли через компанию. Chainalysis утверждают, что Bitzlato получила 206 млн. долларов от даркнет-торговых площадок, 224 млн. долларов от различных мошеннических кошельков, и 9 млн. долларов от криптоадресов вымогательских группировок.

Вторая фирма, Garantex, в 2021 году провела через свою фирму подозрительные транзакции на сумму свыше 645 млн. долларов. По данным Chainalysis, Garantex получила около 10 млн. долларов от кошельков владельцев вирусов-вымогателей[1].

Причиной этого может быть то, что преступники пользуются только проверенными услугами. Chainalysis, одна из ведущих компаний в области блокчейн-анализа, которая предоставляет программное обеспечения для правового соответствия и проведения собственных исследований банкам, криптобизнесам и государственным учреждениям, в своем сайте, указали, что эти адреса могут быть рассмотрены более подробно и существует возможность их определения.

---

[1] Chainalysis: 55% незаконно полученных криптовалют отмываются через 5 сервисов. – URL: https://bits.media/chainalysis-55-nezakonno-poluchennykh-kriptovalyut-otmyvayutsya-cherez-pyat-servisov/ (дата обращения: 10.03.2022).

Исходя из изложенного, можно сделать вывод, что преступления в сфере высоких технологий появились практически сразу же, как только появились и сами компьютерные технологии. Менее чем за 35 лет с момента появления компьютерных технологий, преступная среда адаптировала их для совершения противоправных деяний. С каждым днем, методы и средства совершения данных видов преступлений становятся все совершенней. К тому же, объектами противоправных деяний могут стать не только обычные пользователи сети Интернет, но даже целые организации, среди которых международные банковские системы, что говорит о том, что данный вид преступлений является опасным явлением. При этом, судя по статистике, раскрываемость преступлений, совершаемых с использованием информационно-телекоммуникационных технологий крайне мала.

§2. Влияние фактора социальной напряженности на состояние преступности с использованием компьютерных и телекоммуникационных технологий

К уже имеющимся, активно влияющим факторам, указанным в первой части настоящего исследования, способствующим совершению преступлений посредством использования компьютерных, информационных и телекоммуникационных технологий, добавился и еще один, из-за которого компьютерная преступность возросла в разы. Появление данного фактора никто не мог предсказать. Данный фактор возник ввиду введенных изменений в жизнедеятельность как отдельных граждан, так и целых организаций в связи с установленными государствами ограничениями из-за распространения новой коронавирусной инфекции Covid-19. Эти изменения возникли ввиду смены привычного ритма жизни, переходом на удаленную работу, введением режима саморегулирования, ограничением свободного передвижения, приостановление деятельности ряда организаций сферы услуг, досуга и т.д.

Конечно же, есть и положительная сторона. Указанные ограничения послужили большим стимулом для дальнейшего развития цифровых

технологий, образовательной деятельности, финансового сектора, интенсивной интеграции ряда других сфер социально-экономической деятельности, а главное возникновение пристального внимания общественности к проблеме компьютерных преступлений, и появление в разных организациях, специалистов по кибербезопасности.

Довольно точно высказался основатель и руководитель Давосского экономического форума, Клаус Шваб[1]: «Мы должны подумать о том, как структурировать, спроектировать нашу жизнь в период после пандемии. И здесь подойдет слово «Перезагрузка», ведь нам ясно – к старой норме возврата не будет. За прошедшие 15 недель пандемии, человечество сделало для цифровой трансформации больше, чем за последние 15 лет».

Ввиду введенных государствами, ограничительных мер из-за распространения новой коронавирусной инфекции Covid-19, отдельные лица, организации и государства, ощутили сильную зависимость от стабильной работы электронных почт, систем дистанционного обучения, каналов связи, сервисов банка, и иных форм предоставлений онлайн услуг. Многие организации перешли на удаленный режим работы, в основном осуществляя свою трудовую деятельность через программы для видеоконференций и облачных сервисов по хранению информации. Также, в режим удаленной работы перешли все отрасли экономики, образовательная и финансовая деятельности, включая розничную торговлю. В связи с вышеуказанными обстоятельствами, возникли риски, связанные с возможностью посягательства на цифровые данные. Это является не только российской, но и мировой тенденцией.

Среди указанных выше факторов, способствующих к совершению преступлений в сфере информационных и телекоммуникационных технологий, появились и дополнительные факторы:

- рост объема коммуникаций в сетях Интернет, как отдельными лицами, так и структурированными организациями и государственными

[1] Клаус Шваб: пандемия как трамплин. – URL: https://stolcom.com/klaus-shvab-pandemiya-kak-tramplin/ (дата обращения: 10.03.2022).

органами. А также увеличение продолжительности времени, в котором пользователи проводят в сетях Интернет. Следует отметить, что среди прочего также увеличилось число пожилых людей, которые недостаточно информированы о противоправных действиях в сетях Интернет. Они то и являются наиболее уязвимыми мишенями для компьютерных мошенников, из-за чего увеличиваются факты вымогательств, распространения вредоносных программ и т.д.;

- переход значительной части организаций в удаленный режим работы при отсутствии опыта управления и линейного персонала обученного работе с информационными и телекоммуникационными технологиями. Примерами проблематики в данном направлении, стало широкое распространение передачи важной информации, паролей и логинов учетных записей, файлов, содержащих персональные данные и т.д. через электронную почту, социальные сети и прочие средства общения;
- неподготовленность бизнес-процессов многих организаций для перевода своих работников на удаленный режим работы, что создает условия распространения фишинговых почтовых рассылок. При открытии таких рассылок запускается вредоносный код, который позволяет третьим лицам, втайне от жертвы, пользоваться его компьютером. Такие рассылки осуществляются якобы от имени начальства организации. В текст своего сообщения, мошенники, для способствования своего успеха, вкладывают свои навыки «социальной инженерии», что препятствует принятию сбалансированного решения путем ограничения во времени от лженачальства, и искусственному созданию тревоги;
- активное запугивание населения об угрозах, связанных с распространением вируса Covid-19, для рекламы поддельных лекарств, антисептиков, средств индивидуальной защиты, медицинских консультаций и онлайн-диагностики;
- действия государств, направленные на защиту занятости населения во время пандемии оказались недостаточно эффективными, и огромные массы людей были лишены своих источников дохода. В возникших условиях, многие

люди остались с острой нуждой к обеспечению денежными средствами своей семьи.

Коронавирусная инфекция Covid-19, способствовала сильному росту криминальной активности, особенно в рассматриваемой нами сфере. Наличие возможности к получению легкой наживы, заставило многих людей, ранее бывших обычными работниками, встать на путь киберпреступлений. Кроме роста числа киберпреступников, также преобразились способы совершения противоправных действий в сетях Интернет.

Необходимо отметить основные изменения в способах совершения преступлений, совершаемых с использованием компьютерных, информационных и телекоммуникационных технологий в период пандемии Covid-19:

1. Усовершенствование способов совершения преступлений, посредством «социальной инженерии», направленных на получение конфиденциальной информации от клиентов финансово-кредитных организаций посредством телефонной связи под различными предлогами. Основные моменты при реализации компьютерных преступлений не потерпели серьезных изменений. Однако теперь в мошеннических схемах изменилась «обертка» под современные события:

- телефонный звонок от социальных работников с предложением оказать содействие в получении государственных пособий, которые просят указать свои персональные данные;
- звонок от медицинской организации, сообщающий о родственнике, который был госпитализирован с коронавирусом, и возможность подключения устройства искусственного дыхания за деньги;
- штрафы за нарушение карантина и т.д., к убедительности этого приводит введение режима самоизоляции и наличие сотрудников в режиме дистанционной работы.

2. Активное распространение сообщений с вредоносными программами, маскирующихся под тематику Covid-19. Вредоносные программы, содержащиеся в сообщениях, выполняют скрытые от жертвы действия, нацеленные на хищение личных данных граждан.

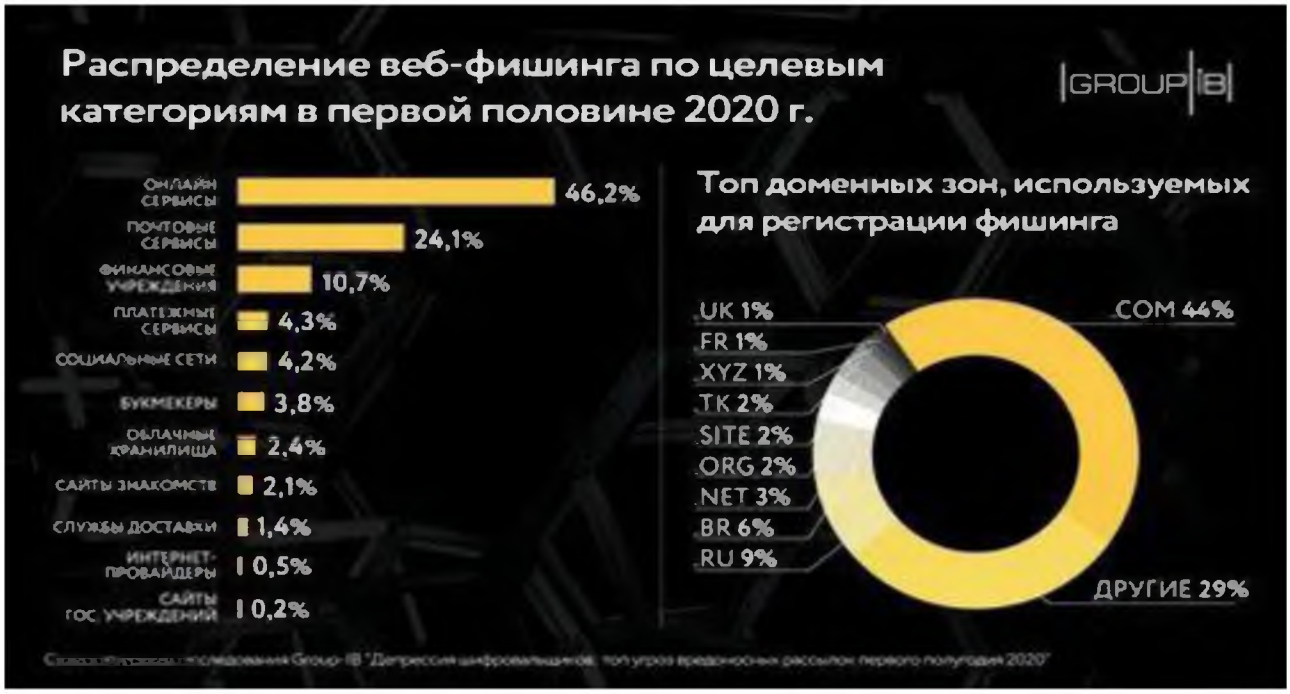
Во время пандемии, было зафиксировано множество попыток, завладения персональными данными жертв, якобы для оказания помощи в оформлении государственных пособий, помощи в компенсации за неиспользованные авиабилеты из-за отмены рейсов, продажа покупателям некачественных медицинских изделий (не соответствующие нормам качества, медицинские маски, перчатки, неисправные инфракрасные термометры или предметы конструктивно схожих с медицинскими изделиями и т.д.).

Случаи покупки широко распространены, и схемы обмана жертв уже довольно примитивны: пользователь отправляется на созданную мошенниками фишинговый сайт, где необходимо ввести личные данные и данные с банковской карты.

В частности, сведения о распределении фактов фишинга по целевым категориям в первой половине 2020 г. представлено на диаграмме №1.

Диаграмма 1.

Распределение фишинга по целевым категориям в первой половине 2020 г. (по данным компании Group-IB)



Также, имели место факты получения по электронной почте сообщений, в которых содержались ложное уведомления, якобы от «оперативного штаба по борьбе с коронавирусом». Такое письмо приходило к пользователям с вирусом внутри, при открытии которого, компьютер «заражался».

Выявлены факты размещения информации в социальных сетях о государственной выплате за неиспользованные медицинские услуги по полису ОМС. Для этого жертве отправлялась ссылка на предложенный сайт, чтобы заполнить форму и узнать размер предполагаемой «компенсации». После этого пользователю предлагается указать номер своей банковской карты, для перевода денег, после чего мошенники получают возможность распоряжения денежными средствами жертвы.

Еще один вид мошенничества возник из-за ограничений передвижения в рамках населенного пункта, а точнее за штрафы, связанные с их нарушением. Это вдохновило мошенников к созданию программ для телефонов, которые позволяют определить, на какое расстояние можно отходить от дома. В данных программах, также требовались данные банковской карты, которые впоследствии использовались для вывода с карты жертвы денег.

Вывод огромного числа работников в «запас» с неопределенным сроком, стало одной из основных причин роста компьютерного мошенничества, совершаемое якобы от лица агентств по трудоустройству. Основой для реализации мошеннической схемы стала рассылка приглашения на «собеседование с работодателем» через Zoom-конференцию, которая перенаправляла жертву на «фишинговый» сайт.

Во время майских праздников 2020 г. было опубликовано видео о том, как правильно носить маску. Казалось бы, ничего плохого в этом нет, однако данное видео распространяло вредоносный вирус «Ginp», который загружался под видом программы для просмотра самого ролика. При первом же запуске программы, устанавливалось вредоносное ПО, с помощью которого злоумышленнику становилось возможным удаленно управлять компьютером жертвы[1].

3. Колоссально популяризированные, во время пандемии Covid-19, программы, для онлайн конференций оказались весьма уязвимы для внедрения в них различных вредоносных программ и вирусов. Так, например в той же

[1] Троян Ginp зарабатывает на коронавирусе. – URL: https://teletype.in/@kasperskydaily/RObekypzw (дата обращения: 12.03.2022).

программе «Zoom» обнаружены серьезные уязвимости, благодаря которым злоумышленники могли модифицировать программу и получить полный контроль над системой жертвы. Ввиду того, что для работы пользователь мог сутками держать программу в активном состоянии, киберпреступники получали возможность доступа к информационной системе. После этого они с помощью специальных программ повышали свои права доступа к информационной системе и шифровали важные для работы файлы и документы, при этом оставляя сообщения с требованиями выкупа за разблокировки системы.

Так, в марте 2020 г., специалистами компании Group-IB обнаружена массированная рассылка сообщений в электронные ящики с названием «Бесплатные защитные маски для лица от коронавируса». В сообщении рассылки была обнаружена шпионская программа «HawkEye». Письмо якобы было отправлено менеджером китайской компании Galaxy Electronic Industrial, а покупателями были российские компании, в том числе из энергетического сектора. В письме говорилось, что китайская компания запустила завод по производству медицинских масок, который находится на стадии сертификации продукции во время инвестиций, а сертификация товара содержится во вложении[1].

4. Крайне частым явлением во время пандемии стали услуги, позволяющие игнорировать ограничительные меры из-за новой коронавирусной инфекции. Среди таких услуг появились предложения по онлайн оплате штрафа, наложенного за фиксацию момента нахождения лица в общественном месте без средств индивидуальной защиты, предложения по проведению «обязательного» платного анализа, необходимого из-за контакта с носителем вируса, предоставление фиктивных справок об отрицательном результате тестирования на наличие коронавирусной инфекции, изготовление пропусков для свободного передвижения по населенному пункту и многое

[1] Group-IB: шпионские программы лидируют в почтовых рассылках, паразитирующих на теме коронавируса. – URL: https://www.group-ib.ru/media/covid-phishing-campaings/ (дата обращения: 12.03.2022).

другое. При проверке, документов у лиц, воспользовавшихся данными услугами, устанавливалась недействительность документов. То есть, лицо лишалось и средств, за которые приобрело услугу, и лишалось самого документа, из-за которого лицу также приходилось платить штраф. С середины апреля 2020 г. был зафиксирован большой рост регистрации поддельных сервисов-сайтов, Telegram-каналов и Instagram-аккаунтов, в которых размещалась реклама о продаже пропусков для передвижения по городу по цене от трех тысяч до пяти тысяч рублей[1].

Менее удачно у компьютерных мошенников, получилась схема с обманом жертвы, распространяемое через рассылки в социальных сетях и через СМС-рассылки. В данном варианте, злоумышленники ссылались на якобы решение Федеральной Службы исполнения наказаний о наложении штрафа за нарушение режима самоизоляции или же за нарушение требований ПДД. Указанный штраф потенциальные жертвы должны были оплатить в течение суток, в противном случае в отношении них обещалось завести уголовное дело.

5. Медицинские маски, перчатки, респираторы, антисептики, термометры в первые недели введения мер для ограничения распространения новой коронавирусной инфекции Covid-19 вызвали огромный спрос среди населения. Наличие дефицитного товара снова вызвал предложение со стороны мошенников. По данным Роспотребнадзора, во время пандемии рекламировались «уникальные» предметы, такие как портативный аппарат для очищения воздуха в помещении от возбудителей инфекции коронавируса, фильтрующие воздух, маски от вирусов-возбудителей коронавирусной инфекции или «специальное» мыло от COVID-19 и т.д. Цена таких продуктов была очень высокой, а эффективность не доказана. Данная активность была непродолжительна, в связи с информированием государства о сущности инфекции. Однако число людей, пострадавших от данного вида мошенничества было довольно большим.

---

[1] Преступники начали выдавать «разрешения» раньше официальных властей. – URL: https://dailystorm.ru/rassledovaniya/chto-sluchitsya-esli-kupit-cifrovoy-propusk-v-telegram (дата обращения: 12.03.2022).

Принимая во внимание сохранение вышеприведенных факторов и после окончания действия большинства ограничений, вызванных борьбой с распространением новой коронавирусной инфекции COVID-19 и способствующих росту числа преступлений, совершаемых с использованием в данной сфере информационно-телекоммуникационных технологий, к сожалению, в краткосрочной перспективе мы можем лишь прогнозировать увеличение числа рассматриваемого вида преступлений.

Следует подытожить, что действия злоумышленников в период пандемии коронавируса, в первую очередь взаимосвязаны с переводом огромного числа населения на удаленный способ работы и обучения. Государственные учреждения и коммерческие организации столкнулись с трудноразрешимыми проблемами в обеспечении информационно-телекоммуникационной безопасности, ведь подключение работников, сотрудников и обучающихся к сети осуществлялись через домашние, сетевые маршрутизаторы, с известными, для компьютерных преступников, уязвимостями. По своей сути, демонстрируемый статистикой рост данных видов преступлений напрямую связан именно с ростом числа потенциальных жертв компьютерных преступлений, так как злоумышленники использовали весьма популярные виды совершения преступлений в рассматриваемой сфере.

ГЛАВА 2. ВОПРОСЫ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ, СОВЕРШАЕМЫМ С ИСПОЛЬЗОВАНИЕМ КОМПЬЮТЕРНЫХ И ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

§1. Криминологическая характеристика преступлений, совершаемых с использованием информационно-телекоммуникационных технологий

Бесспорно, что развитие информационных технологий в современном мире порождает их повсеместное проникновение во все сферы общественной жизни. К сожалению, этим пользуются не только добросовестные пользователи коммуникационных сетей, но злоумышленники, которые преследуют различные противоправные цели – личное обогащение, дискредитацию граждан и государственных органов, распространение нелегальной информации, идей терроризма и экстремизма.

В Российской Федерации отмечается ежегодный рост преступлений, совершаемых с использованием современных информационно-коммуникационных технологий[1].

Такой быстрый рост преступности требует необходимости повышения эффективности противодействия киберпреступности, что несомненно относится к стратегическим направлениям деятельности органов внутренних дел.

И одним из основных вопросов в данном случае считается усовершенствование действующего законодательства, для того чтобы усилить защиту граждан и общества от противоправных посягательств. Уголовно-правовые запреты должны соответствовать существующим реалиям и обеспечить полностью пропорциональную ответственность за совершение преступных посягательств.

---

[1] Аносов А. В. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: учебное пособие: в 2 ч. М.: Академия управления МВД России, 2019. Ч. 1. С. 157.

В то же время, в условии быстроразвивающихся видов преступности, что особенно актуально для киберпространства, конструкция уголовно правовых норм обязана не просто учитывать складывающуюся криминогенную обстановку, но и, в идеале, заглядывать в будущее, предсказывая в своей фабуле возможные опасные варианты развития методов и средств применения информационно-коммуникационных технологий в незаконных целях.

Например, в целях борьбы с компьютерной преступностью УК РФ предусмотрена ответственность за ряд специальных составов, криминализирующих такие деяния как: неправомерный доступ к охраняемой законом компьютерной информации независимо от способа его совершения, создание, использование и распространение вредоносных компьютерных программ; мошенничество в сфере компьютерной информации, а также нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей[1].

Кроме этого, совершение преступлений с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет») рассматривается в целом ряде составов УК РФ в качестве квалифицирующего или отягчающего наказание признака – ч. 3 ст. 137 «Нарушение неприкосновенности частной жизни», ст. 138 «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений», ст. 228.1 (п. «б» ч. 2, ч. 3, 4, 5) «Незаконное производство, сбыт или пересылка наркотических средств, психотропных веществ или их аналогов, а также незаконные сбыт или пересылка растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества», ст. 282 «Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства» и другие.

Следовательно, можно с уверенностью заявить, что действующими уголовно-правовыми запретами охватываются основные виды противоправных деяний в рассматриваемой сфере.

---

[1] Аносов А. В. Указ. соч. С. 164.

Вместе с этим органами внутренних дел осуществляется работа по обеспечению законодательной защиты новых объектов посягательств в киберпространстве, появление которых является результатом слишком быстрого развития информационных технологий.

В частности, с 01.01.2018 года вступили в силу изменения уголовного закона, устанавливающие ответственность за неправомерный доступ к критической информационной структуре Российской Федерации, а также за создание и распространение компьютерных программ, предназначенных для этих целей (ст. 274.1 УК РФ).

Бесспорно то, что использование вредоносных компьютерных программ в корыстных целях превращает криминальную деятельность в сверхприбыльную. Существующие правила эксплуатации сети Интернет обеспечивают анонимность преступных действий и возможность доступа к значительным материальным ресурсам.

Как следствие, опасность стать жертвами этих деяний в наше время распространяется на всех участников информационно-телекоммуникационной сферы, включая владельцев банковских дебетовых карт и мобильных телефонов[1].

Однако далеко не всегда киберпреступления совершаются лишь с использованием специальных познаний в области информационно-телекоммуникационных технологий.

Следует отметить, что множество преступлений в данной сфере совершается с использованием методов «социальной инженерии», то есть неправомерного доступа к информации или системам хранения информации без использования технических средств. Технология основана на использовании слабостей человеческого фактора и, к сожалению, является достаточно эффективной.

Злоумышленник получает информацию, например, путем сбора информации об объекте атаки, с помощью обычного телефонного звонка или

[1] Гаврилин Ю. В. Расследование неправомерного доступа к компьютерной информации: дис. ... канд. юрид. Наук. М., 2000. С. 105.

путем проникновения в организацию под видом ее служащего. Преступник также может позвонить человеку, являющемуся пользователем кредитной карты (под видом сотрудника службы поддержки или службы безопасности банка), и выведать пароль, сославшись на необходимость решения небольшой проблемы в компьютерной системе или с банковском счетом, зачастую дезинформируя о его блокировке. И очень часто этот трюк срабатывает.

По сути, известный нам фишинг – также включает в себя технику «социальной инженерии», направленная на получение конфиденциальной информации путем обмана или недомолвки важных информационных деталей. Обычно злоумышленник посылает посредством e-mail, сообщение, под видом официального письма банка или платежной системы, требующего «проверки» определенной информации, или совершения определенных действий. Это письмо обычно содержит ссылку на фальшивую web-страницу, имитирующую официальную, с корпоративным логотипом и содержимым, и содержащую форму, требующую ввести конфиденциальную информацию – от домашнего адреса до пин-кода банковской карты.

Социальная инженерия также используется для распространения троянских коней: эксплуатируется любопытство, либо корыстные цели.

Злоумышленник отправляет e-mail, sms-сообщение или сообщение в мессенджере, во вложении которого содержится, например, важное обновление антивируса. Также, это может быть выгодное предложение о покупке со скидкой или сообщение о фиктивном выигрыше с приложенной ссылкой при переходе по которой на устройство пользователя скачивается вредоносная программа.

В результате указанных действий злоумышленник получает доступ к устройству и личным данным жертвы, а также возможность управлять ими в своих целях.

Такая техника остается эффективной, поскольку многие пользователи без раздумий кликают по любым вложениям или гиперссылкам. Особенно это актуально в связи с глобальной цифровизацией общества, которая затрагивает и социально уязвимые слои населения, например, пожилых людей,

испытывающих сложности при освоении современной техники, что увеличивает риски оказаться жертвой мошенников.

Учитывая данное обстоятельство, а также то, что в Российской Федерации борьба с преступностью рассматривается как комплексное явление, включающее в себя не только поиск виновных, привлечение их к ответственности, но и меры, направленные на предупреждение преступлений, было принято решение о проведении правоохранительными органами среди населения правового просвещения, направленного на разъяснение широким слоям населения основ информационной безопасности[1].

Говоря о социально уязвимых группах нельзя не отметить, что очень часто сеть «Интернет» используется злоумышленниками в отношении несовершеннолетних и молодежи.

С развитием информационных технологий и глобальной сети «Интернет» несовершеннолетние активно общаются посредством социальных сетей, которые в свою очередь стали одним из инструментов и способов совершения преступлений. Стремительное распространение информации в сети не всегда позволяет оперативно отслеживать безопасность общения.

Органами прокуратуры Российской Федерации выявляются многочисленные Интернет-сайты, содержащие призывы к совершению суицидов, детальное описание механизмов причинения вреда здоровью и фотографии с демонстрацией способов совершения самоубийства. Ряд совершенных несовершеннолетними в прошлом году суицидов связан с деятельностью так называемых «групп смерти», в сети «Интернет», что вызвало широкий общественный резонанс и повлекло уголовное преследование создателей таких сообществ.

Названные группы, имеющие наименования «Синий кит», «Тихий дом» и иные, предлагают подросткам вступить в игру, длящуюся 50 дней, имеющую несколько уровней. Их преодоление возможно при условии успешного

---

[1]Дворецкий М. Ю. Преступления в сфере компьютерной информации. Научно-практический комментарий к главе 28 Уголовного кодекса Российской Федерации. Тамбов, 2017. С. 324.

прохождения подростками 50 заданий, среди которых причинение себе резаных ран на руках и иные действия, причиняющие вред здоровью и жизни ребенка. При виртуальном общении на несовершеннолетнего оказывается психологическое давление, для облегчения выполнения заданий его убеждают в ненужности, отсутствии любви близких, соответственно бессмысленности жизни. После этого вовлеченный в «игру» подросток должен совершить суицид.

С целью предотвращения таких инцидентов и исключения возможности доступа несовершеннолетних к информации суицидальной направленности и иной запрещенной законом, создан Единый реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, содержащих сведения, распространение которых в Российской Федерации запрещено.

Генеральная прокуратура Российской Федерации принимает активное участие в выявлении такой информации и осуществлению ее блокировки, во взаимодействии как с уполномоченными государственными органами, так и администрацией различных сетевых ресурсов.

Кроме того, упомянутые события послужили основанием введения с 07.06.2017 года, в УК РФ правовой нормы, предусматривающей ответственность за склонение к совершению самоубийства, в том числе с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет»).

В целом имеющиеся данные не оставляют сомнений в том, что преступность очень быстро приспосабливается к меняющимся условиям. И очевидно, что преступники будут расширять свою деятельность в рамках глобальной виртуальной криминальной сети, не знающей ни границ, ни юрисдикции. А в силу возможности анонимизации в Интернете, расследование таких преступлений процесс сложный и зачастую не быстрый[1].

Наиболее сложные уголовные дела обычно связаны с крупными преступными группами, которые занимаются целевыми атаками, кражами

[1] Мещеряков В. А. Основы методики расследования преступлений в сфере компьютерной информации: дис. ... д-ра юрид. наук. Воронеж, 2001. С. 255.

денег через Интернет-банк или мобильные приложения финансовых организаций. Преступники в этих случаях уделяют большое внимание тому, как скрыть свою личность – используют несколько цепочек серверов для доступа к ресурсам, применяют шифрование, постоянно переписывают программы для атак.

К сожалению, зачастую по единственному инциденту установить злоумышленников в этом случае не удается. Только по нескольким эпизодам собирается материал, с которым можно работать, но даже тогда процесс поиска может затянуться. Длительное время, учитывая специфику киберпреступлений, также требуется для составления доказательной базы.

Другую сложность представляет то, что в таких преступных группах роли четко распределены, поэтому преступление от начала до конца совершается разными людьми. Лидер группы нанимает исполнителей определенных задач: настроить сервер, написать и распространить вредоносную программу, обеспечить защиту вредоносного софта от антивирусов и брандмауэров. Причем такими людьми могут оказаться и обыкновенные студенты, интересующиеся информационными технологиями и иногда даже не подозревающие, что участвуют в преступной группе. Как правило, с человеком связывается аноним и предлагает деньги за определенную работу, например, создание программы, настройка сервера и т.п. Зачастую организатор поясняет исполнителю, для чего будет применяться результаты заказанной работы. В то же время, к примеру, при разработке программы, перехватывающей данные, исполнитель может понимать, что она может быть использована в преступных целях.

Иногда такие программы приобретаются у третьих лиц, и автор не информирован о том, как преступники будут ее использовать, для перехвата каких именно данных. С другой стороны, программист, пишущий для «софта» защиту от антивирусов – очевидно должен осознавать, что для легальных целей такие действия не совершаются. Например, показательно в этом отношении раскрытое в Российской Федерации уголовное дело в отношении членов преступного сообщества, которые разработали вредоносное программное

обеспечение и создали частную виртуальную сеть для получения финансовой выгоды.

Их программы позволили незаконно направлять в Центральный Банк Российской Федерации электронные файлы с реестром платежей в различных суммах на большое количество счетов, подконтрольных злоумышленникам. Кроме того, на приобретенные ими банковские карты перечислялись похищенные денежные средства с целью их дальнейшего обналичивания.

Подготовка к совершению данных незаконных действий заняла у преступников более года, и такая тщательность позволила им совершить хищение свыше 1,2 миллиарда рублей (20 миллионов евро). При этом вербовка членов данной преступной организации, их дальнейшее взаимодействие и осуществление своих преступных планов осуществлялись через сеть Интернет, большинство преступников не были лично знакомы и имели место жительство в различных странах мира, никогда напрямую не контактировали. Необходимо отметить, что сегодня все большее развитие получает рынок аренды вредоносного программного обеспечения. Настоящие программисты составляют лишь определенный процент киберпреступников[1].

Остальные – злоумышленники, которые приобрели ту или иную программу и используют ее в корыстных целях. Причем интерфейсы многих таких программ уже почти не отличаются от офисных программ и интуитивны для освоения. Не случайно популярный сегодня вариант кибератак – внедрение вредоносного программного обеспечения в сеть в автоматическом, заскриптованном режиме, когда преступнику достаточно запустить программу и ждать результатов.

Создание или модификация таких программ под специальные задачи, обозначенные заказчиком, также является одним из видов получившего в последнее время широкое распространение в Интернет-пространстве явления, которое получило наименование «преступление как услуга». За определенную плату так называемые «специалисты» совершат DDoS-атаку на указанные

[1] Краснова Л. Б. Компьютерные объекты в уголовном процессе и криминалистике: дис. ... канд. юрид. наук. Воронеж, 2015. С. 11.

серверы, или предоставят ботнет (скрытая программа для управления «взломанным» устройством) для незаконных целей[1].

Развитие информационных технологий позволяет преступникам создавать новые механизмы совершения преступных деяний, которые сложны не только для обнаружения, но и для ликвидации как самих вредоносных программ, так и их последствий.

Например, уникально с точки зрения способа было имевшее место в Российской Федерации преступление, связанное с хищением денежных средств из банка. С помощью вредоносной программы злоумышленники получили доступ к автоматизированному рабочему месту клиента данного банка, и доступ к каждому компьютеру внутри организации, в том числе и в филиалах. Для этого на одном компьютере в сети был запущен «компьютерный червь», который работал исключительно в оперативной памяти компьютера. То есть представлял собой так называемую «бестелесную программу» (fileless). Другими словами, преступники создали контролируемую бот-сеть внутри банка, в которой если хотя бы один зараженный компьютер будет включен, то он снова и снова будет распространять вирус в сети компании. Очевидно, что в таком случае, без принудительной одновременной остановки всей компьютерной сети банка избавиться от вредоносной программы было невозможно. И легко представить ущерб от такой остановки[2].

Специфика сложности установления лиц, совершающих преступления в информационно-коммуникационных сетях, накладывает свои ограничения и при расследовании преступлений. Зачастую правоохранительные органы, осуществляя производство по уголовному делу о преступлении, совершенном группой лиц, в случае установления одного из соучастников, не стремятся немедленно задержать его, а могут продолжать фиксировать его дальнейшие

---

[1] Батурин Ю. М. Компьютерные правонарушения: криминализация, квалификация, раскрытие / Ю. М. Батурин, А. М. Жодзишский // Советское государство и право. 1990. № 12. С. 88.

[2] Гаврилин Ю. В. Особенности криминалистической характеристики неправомерного доступа к компьютерной информации // Известия Тульского государственного университета. Сер.: Современные проблемы законодательства России, юридических наук и правоохранительной деятельности. 2020. Вып. 1. С. 195.

действия с целью выявления и задержания остальных участников преступного сообщества.

Большое внимание со стороны государственных органов власти уделяется вопросам возмещения ущерба, причиненного киберпреступлениями. В Российской Федерации функционирует Федеральная служба по финансовому мониторингу (Росфинмониторинг), которая является федеральным органом исполнительной власти, осуществляющим функции по противодействию легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения.

При этом, органы предварительного расследования ориентированы на активное взаимодействие с указанной службой по вопросам предоставлению сведений о суммах, характере и периодах совершения операций (сделок) лицами, причастными к преступным деяниям. Также в настоящее время в Российской Федерации видится перспективным полноценное использование всего ресурса действующих в государственных и частных центрах реагирования на инциденты в сфере компьютерной информации, целью которых является сбор сведений об уязвимостях жизненно важных объектов инфраструктуры.

В частности, был создан подобный Центр реагирования на компьютерные инциденты в кредитно-финансовой сфере. В первый год его существования удалось предотвратить хищения из российских банков на общую сумму более трех миллиардов рублей, а также совместно с правоохранительными органами пресечь деятельность двух организованных преступных групп, уникальных по широте своей преступной деятельности и способам совершения преступлений[1].

На базе указанного Центра создается центр компьютерных экспертиз, что положительно сказывается на эффективности расследования преступлений, совершаемых в рассматриваемой сфере. Также в Российской Федерации

---

[1] Баландюк Р. О. Методика расследования отдельных видов преступлений, совершаемых в сфере интернет-технологий / Р. О. Баландюк [и др.] // Вестник Белгородского юридического института МВД России. 2015. № 1. С. 71.

функционируют специализированные подразделения правоохранительных органов по выявлению и расследованию киберпреступлений, уже не раз доказавшие свою эффективность в борьбе с рассматриваемыми преступными деяниями.

В то же время любые организационные и практические меры, проводимые внутри одной страны, могут быть максимально результативными только при наличии надлежащего механизма международно-правового сотрудничества. В этой связи целесообразно совершенствовать существующие процедуры в части упрощения процедуры взаимодействия, в том числе использования в этой сфере современных информационных технологий.

В связи со складывающейся ситуацией, образовывается вывод, что совместные усилия правоохранительных органов в сфере международного сотрудничества необходимо сосредоточить на выработке более действенных мер, с учетом технического прогресса и возрастающей сложности изобретенных преступных схем.

К сожалению, не всегда уровень такого сотрудничества и скорость обмена информацией позволяет правоохранительным органам действовать быстро и адекватно, используя весь потенциал для борьбы с преступниками.

Например, имел место случай, когда при осуществлении правоохранительными органами Российской Федерации оперативно-розыскных мероприятий, направленных на выявление лиц, совершающих преступления с использованием информационно-коммуникационных технологий в правоохранительные органы иных стран была направлена информация относительно 177 зарубежных пользователей сети Интернет, распространяющих противоправный контент. От правоохранительных органов зарубежных государств поступило всего два ответа[1].

При таких обстоятельствах весьма сложно говорить об оперативном и своевременном раскрытии преступлений и привлечении к надлежащей ответственности лиц их совершающих. При этом Генеральная прокуратура

[1] Атаманов Р. С. Основы методики расследования мошенничества в сети Интернет: дис. ... канд. юрид. наук. М., 2012. С. 146.

Российской Федерации придерживается активной позиции в части развития международного сотрудничества в сфере борьбы с преступлениями, совершаемыми с использованием информационно-коммуникационных технологий. С 2015 года принято участие в 12 мероприятиях по вопросам противодействия преступлениям, совершаемым с применением информационно-коммуникационных технологий и носящим транснациональный характер. В заключение хотелось бы отметить, что новые горизонты информационных технологий уже заставляют задуматься о предстоящих сложностях в работе правоохранительных органов. Уже можно наблюдать повсеместное распространение блокчейн-технологий, не за горами внедрение квантового шифрования и стремительное развитие нейросетей. Наивно было бы предполагать, что изощренные умы не попытаются приспособить и эти достижения человеческой мысли для реализации своих корыстных противоправных целей[1].

Стоит отметить, что в условиях появления новых вызовов криминального сообщества, без малейшего сомнения, использующего отсутствие границ в виртуальном пространстве, правоохранительные органы должны быть на шаг впереди в части международного взаимодействия и прилагать максимально возможные усилия к его совершенствованию. Можно выразить уверенность в том, что лишь совместными действиями существует возможность, если не минимизировать преступную деятельность в киберпространстве, то, самое меньшее, не позволить злоумышленникам избежать установленной ответственности за свои действия.

§2. Предупреждение преступлений, совершаемых с использованием компьютерных и телекоммуникационных технологий

Система мер по предупреждению преступности является одной из сфер социального управления, так как оно предполагает воздействие не только на

[1] Простосердов М. А. Экономические преступления, совершаемые в киберпространстве, и меры противодействия им: дис. ... канд. юрид. наук. М., 2016. С. 102.

детерминанты преступности, но и на причины их роста и развития. Согласно криминологическому учению, предупреждение преступности подразделяют на такие меры как общая и специальная. Общие меры профилактики осуществляются путем проведения информирования населения о потенциальных угрозах в сетях Интернета, а специальные меры направлены на профилактическую работу с лицами, которые ранее совершали преступления. Данное деление весьма условно, так как развитие преступности как социального явления требует от правоохранительных органов применения в своей работе более обширных мер профилактики, которые включают как общую, так и специальную профилактику.

Примером таких мер может служить «Доктрина информационной безопасности Российской Федерации», определяющая национальные интересы России в области безопасности информационной среды. Она ставит перед собой такие цели, как выявление, устранение, ослабление, нейтрализация криминогенных факторов, влияющих на рост преступности в информационном поле[1].

Исходя из особенностей исследуемого вида преступлений, можно выделить основные группы мер их профилактики.

К первой группе мер по предупреждению компьютерных преступлений необходимо отнести правовую, которая включает в себя законодательные нормы, устанавливающие уголовную ответственность за незаконные действия в компьютерной среде. Здесь целесообразно рассмотреть тот факт, что глава 28 УК РФ «Преступления в сфере информационных технологий» отражает действующие законодательные нормы, но с момента введения данной главы в 1996 г., законодателем не было внесено ни одного изменения в статьи данной главы, при этом преступность не стоит на месте, а усовершенствует способы и средства совершения противоправных деяний в данном направлении с геометрической прогрессией.

---

[1] Об утверждении Доктрины информационной безопасности Российской Федерации: указ Президента Российской Федерации от 05.12.2016 № 646 // Собр. законодательства Рос. Федерации. – 2016. – № 50, ст. 7074.

На сегодняшний день действующее законодательство не охватывает все разнообразие преступлений, совершаемых в современной компьютерной среде. К примеру, вышеупомянутая ст. 272 УК РФ в качестве основания для привлечения к уголовной ответственности предусматривает «Неправомерный доступ к компьютерной информации» в качестве оснований, влекущих уголовное преследование, предусматривает уничтожение, блокирование, модификацию или копирование информации, а также нарушение компьютерной системы, компьютерной системы или их сети.

Хотелось бы отметить, что законодатель допустил серьезную ошибку, не добавив еще и такое основание как «несанкционированное ознакомление», ведь порою злоумышленнику достаточно увидеть и прочитать информацию, для того, чтобы информация потеряла свою ценность или для того чтобы в дальнейшем использовать информацию без какого-либо копирования.

Кроме того, ряд санкций не соответствует такому принципу уголовного закона как справедливость. Примером, в данном случае, служит ст. 273 УК РФ «Создание, использование и распространение вредоносных программ для ЭВМ, сети ЭВМ, их сетей». Данная статья предусматривает ответственность уже на стадии создания вредоносной программы, независимо от того, использовалась эта программа или нет. Исходя из текста ст. 273 УК РФ, уже наличие начальных текстов вирусных программ является основанием для привлечения к ответственности.

Хотя создание вредоносного ПО само по себе не может привести к общественно опасным последствиям, а порою, оно необходимо для обучения специалистов в сфере информационных технологий способам противодействия и нейтрализации подобного вида вирусов.

Для вменения ст. 274 УК РФ «Нарушение правил эксплуатации ЭВМ и сети ЭВМ, их сетей» необходимо наличие инструкций и правил, определяющих порядок работы, которые должны быть установлены уполномоченным лицом и доводиться до сотрудников и пользователей. Данная статья распространяется только на локальные сети организаций, и фактически, применение данной статьи невозможна, при совершении преступлений в глобальной сети Интернет.

Несовершенства действующего законодательства порождают не только проблемы, которые затрудняют расследование данного вида преступлений, но и их предупреждение.

Наглядно они выглядят следующим образом:

- неоднородность и отсутствие единого механизма следственной и судебной практики. Так, на сегодняшний день Верховным судом РФ так и не даны разъяснения по вопросам применения статей о компьютерных преступлениях. Приговоры и решения судов по однотипным делам расходятся не только в вопросах квалификации, но и в определении размеров наказания;
- отсутствие современных методических рекомендаций по расследованию подобных преступлений, и, как следствие, низкий уровень специалистов правоохранительных органов, занимающихся расследованием данной категории преступлений.

Следует отметить, что среди факторов, которые действительно способны в настоящее время сдерживать рост преступлений, совершаемых с использованием информационных и телекоммуникационных технологий, на первый план выходит формирование убежденности в способности правоохранительных органом обеспечить безопасности компьютерной среды. Потенциальный преступник должен осознавать высокую вероятность быть обнаруженным и понести наказание за содеянное. Ввиду этого, важным элементом профилактики преступлений в сфере компьютерных технологий является проведение целевых мероприятий и распространение информации об успешной борьбе с преступностью в сфере компьютерной информации[1].

Также, необходимо признать, что жертва является значительным элементом механизма преступления. Исходя из этого, повышению эффективности предупреждения преступлений в рассматриваемой сфере способствуют меры профилактики потенциальных жертв преступлений, совершаемых с использованием информационных и телекоммуникационных технологий.

---

[1] Батурин Ю. М. Проблемы компьютерного права. М., 2018. С. 102.

Кроме того, в настоящей системе предупреждения преступлений, совершаемых с использованием информационных и телекоммуникационных технологий существует довольно крупное упущение – недостаточное внимание уделяется изучению личности несовершеннолетнего преступника.

С распространением глобальной компьютерной сети несовершеннолетние в Российской Федерации получили широкие возможности, поэтому особое внимание следует уделить предупреждению противоправных действий среди подростков.

С целью проведения комплексных мероприятий по профилактике преступлений в сфере компьютерной информации, в общеобразовательных учреждениях, необходимо ввести изучение «Основ Кибербезопасности», для разъяснения подросткам о повышенной социальной опасности преступлений в сфере компьютерной информации, ознакомление с уголовной ответственностью и наказаниями за совершение данного вида преступлений.

К сожалению, необходимо признать, что большинство компьютерных преступлений происходит на предприятиях и в организациях плохой проверки и обучения персонала, явных уязвимостей в системе защиты и недостаточной конфиденциальности.

Анализ материалов уголовных дел позволяет сделать вывод, что к таким случаям нередко приводят такие причины и условия, способствующие совершению компьютерных преступлений, как:

1. неконтролируемый доступ сотрудников к панели управления (клавиатуре) компьютера, которая используется как самостоятельно сотрудниками, так и в качестве рабочей станции для удаленной передачи информации первичных бухгалтерских документов при осуществлении финансовых операций;

2. неконтролируемые действия обслуживающего персонала, позволяющие преступнику свободно использовать рабочий компьютера как орудие совершения преступления;

3. эксплуатация программного обеспечения с низким уровнем защиты, которое не обеспечивает необходимый уровень защиты управления;

4. отсутствие уровней доступа сотрудников к документам серьезной финансовой отчетности, в том числе к документам в виде машинной информации, позволяющее любому сотруднику, в том числе и новому работнику иметь доступ ко всей документации организации;

5. простота паролей и кодов доступа к рабочей станции и к ее программному обеспечению, не обеспечивающая способствующая легкому доступу к ЭВМ обслуживающего персонала;

6. отсутствие должностного лица, отвечающего за режим секретности и конфиденциальности частной или коммерческой информации и ее безопасности в части защиты средств компьютерной техники от несанкционированного доступа.

Крайние две причины скорее носят виктимологический характер, что снова подтверждает все возрастающую значимость фактора жертвы, наряду с другими детерминантами совершения компьютерных преступлений.

Помимо организационных и управленческих мер, меры технического характера (аппаратные, программные средства) также могут играть важную роль в борьбе с компьютерными преступлениями.

Аппаратные методы предназначены для защиты компьютерной техники от нежелательных физических воздействий и закрытия возможных каналов утечки конфиденциальной информации. К ним относятся источники бесперебойного питания, устройства экранирования аппаратуры, шифрозамки и устройства идентификации личности.

Методы программной защиты предназначены для защиты самой информации, путем использования разнообразных методов шифрования данных. Практика показывает, что современные методы шифрования позволяют надежно скрыть смысл сообщений.

Исходя из вышеизложенного, можно спрогнозировать дальнейший рост компьютерной преступности в ближайшем будущем, который обусловлен такими факторами, как:

1. стремительное увеличение числа владельцев компьютеров и Интернет-пользователей;

2. легкомысленное отношение руководителей к вопросу информационной безопасности и защите информации;

3. снижение эффективности нынешних технических средств защиты программного обеспечения, против развивающихся методов и средств совершения преступлений, в сфере информационных и телекоммуникационных технологий;

4. увеличение количества безналичных операций с использованием различных финансовых платежных систем, а также расширение обмена информацией, заключения договоров и других операций без надлежащего контроля;

5. более широкое применение в уголовной деятельности современных технических средств, в том числе компьютеров;

6. низкий уровень познаний правоохранительных органов, в борьбе против информационных и телекоммуникационных преступлений.

Нельзя оставить без внимания и тот факт, что в некоторых случаях борьба с вышеуказанными факторами приводит не только к решению проблемы, но и к появлению новых факторов. Например, поспешные указания руководителей организаций заменить старое программное обеспечение более современным программным обеспечением могут привести к большим негативным последствиям. Возможно и такое, что новое программное обеспечение имеет множество технических недостатков, которые обнаруживаются и устраняются только при использовании таких программ. В связи с этим становиться вопрос о том, какие же программы лучше всего себя зарекомендовали и что необходимо приобретать для эффективной защиты от компьютерных преступлений. Для получения ответа на данные вопросы, владельцы крупных фирм и организаций усиливают свое сотрудничество в области обмена опытом по борьбе с данным видом преступлений[1].

Таким образом, можно наблюдать рост международного опыта по борьбе с преступлениями, совершаемыми с использованием информационн-

[1] Цирлов В. Л. Основы информационной безопасности автоматизированных систем. М., 2018. С. 56.

телекоммуникационных технологий. С целью обмена опытом и консолидации усилий по борьбе с новым видом преступности правоохранительными органами проводятся международные семинары, результаты которых обычно преобразуются в совместно разработанный и утвержденный план действий по предупреждению данного вида преступлений. Задачами таких форумов являются обсуждение широкого круга актуальных проблем глобализации информационных систем и их влияние на формирование информационного общества, разработка совместных мероприятий по обеспечению информационной безопасности.

Среди таких мероприятий, в качестве основных задач можно отметить:

- разработка порядка взаимодействия правоохранительных и других заинтересованных министерств и ведомств на международном уровне, а также обмен информацией в борьбе с использованием высоких технологий в преступных целях;
- проведение научно-практических конференций с участием практических работников по вопросам выявления, предупреждения и расследования преступлений в сфере высоких технологий;
- разработка методических рекомендаций по выявлению, предупреждению и раскрытию преступлений в сфере высоких технологий;
- рекомендации подразделениям по расследованию преступлений в сфере высоких технологий в экспертно-криминалистических учреждениях;
- разработка программ обучения кадров, специализирующихся на работе в сфере высоких технологий.

Подводя итоги данной главы, необходимо отметить, что реализация мер по предупреждению преступлений, совершаемых с использованием информационных систем, компьютерных и телекоммуникационных технологий, может занять большое количество времени и, однозначно, потребует крупных затрат государства. При этом, кроме самого предупреждения, законодательным органам также рекомендуется усовершенствовать имеющиеся отношения по эффективному взаимодействию в области международной борьбы с компьютерными преступлениями, так как

само осознание злоумышленниками того, что за их противоправные действия, даже на территории иного государства, наказания не избежать, является самостоятельным фактором предупреждения данных видом преступлений.

ЗАКЛЮЧЕНИЕ

Всех нас, как и многих людей в мире окружают технологии цифрового мира. Это может быть телефон, ноутбук, смарт-часы или целый «умный дом». Все существующие технологии, на сегодняшний день, в своем развитии, встали на путь компьютеризации, в каждой технике современного быта появляется свой процессор, ведь это в разы увеличивает удобство эксплуатации аппарата.

Так, техника, оснащенная процессором обязательно примеряет на себе приставку «умный», что в наше время безусловно повышает статусность техники и, соответственно, статус ее владельца. Многие люди отказываются от надежной, но старой техники в пользу новых, заполоненных электроникой, девайсов.

Основная отличительная особенность «умных» технологий состоит в том, что все они, в качестве одной из своих обязательных признаков, должны быть оснащены доступом к глобальной сети Интернет, для удаленного, комфортного и энергоэффективного управления техники самим владельцем.

Данная тенденция компьютеризации техники происходит практически повсеместно, однако в погоне за высокими технологиями люди, как правило, даже не задумываются о том, что приобретаемая ими электроника, может быть использована в дальнейшем, как орудие или средство совершения противоправных действий в отношении самих же людей.

Отметим, что в реализации данного исследования нами были выявлены содержания и формы реализации преступных деяний с применением компьютерных технологий и телекоммуникационных сетей, анализ теоретических и практических проблем их правового регулирования.

Так, в первой главе настоящей дипломной работы были рассмотрены преступления, в информационной сфере, совершенные с использованием компьютерных и телекоммуникационных технологий, в рамках того, какие угрозы представляет данный вид преступлений, рассмотрены преступные инциденты, демонстрирующие виды компьютерных преступлений и потенциальный размер ущерба, который может быть нанесен.

Также, в рамках данной главы был изучен период, когда в России были введены ограничительные меры из-за распространения новой коронавирусной инфекции Covid-19. Данный период был выбран в качестве рассматриваемого ввиду того, что с 2019 по 2021 гг., был зафиксирован крупный рост компьютерных преступлений. Увеличению числа рассматриваемого вида преступлений способствовало множество факторов, которые возникли именно из-за ограничительных мер. Так, были изучены наиболее регистрируемые факты преступлений в сфере компьютерных технологий, установлены способы, методы и тактика поведения злоумышленников, а также отражена статистика по числу совершаемых, преступлений в сфере информационно-телекоммуникационных технологий, что позволяет ясно увидеть общую картину роста данных видов преступлений.

Во второй главе нами была рассмотрена криминологическая характеристика преступлений совершаемых с использованием информационно-телекоммуникационных технологий в России, рассматриваются способы противодействия данным видам преступлений и выдвигаются рекомендации по борьбе с преступлениями в сфере компьютерных технологий.

Также, в рамках данной главы изучается вопрос предупреждения преступлений, связанных с информационными и телекоммуникационными технологиями. Указываются конкретные причины и условия, способствующие совершению компьютерных преступлений. Как уже было отмечено, именно предупреждение является наиболее эффективным способом борьбы с данным видом преступлений.

Стоит также добавить, что помимо указанных во второй главе настоящей работы мер, по предупреждению компьютерных преступлений, представляется целесообразным проведение профилактических бесед и семинаров о компьютерной преступности, преступлениях в сети Интернет и уголовно-правовой ответственности за них в средствах массовой информации, школах, высших учебных заведениях страны, а также печать на страницах наиболее популярных журналов, статей на тему информационной и телекоммуникационной безопасности, с целью профилактического воздействия

на потенциальных жертв, ввиду того, что данному виду преступлений подвержены практически все население Российской Федерации.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ:

I. Нормативные правовые акты и иные официальные документы

1. Конституция Российской Федерации: принята всенародным голосованием 12 декабря 1993 г. с учетом поправок, внесенных Законом Рос. Федерации о поправках к Конституции Рос. Федерации от 1 июля 2020 г. № 11-ФКЗ // Собр. законодательства Рос. Федерации. – 2020. – № 31, ст. 4398.

2. Уголовный кодекс Российской Федерации: федер. закон Рос. Федерации от 13.06.1996 г. № 63-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 24 мая 1996 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 5 июня 1996 г. // Собр. законодательства Рос. Федерации. – 1996. – № 25, ст. 2954.

3. О национальной платежной системе: федер. закон Рос. Федерации от 27 июня 2011 г. № 161-ФЗ // Собр. законодательства Рос. Федерации. – 2011. – № 27, ст. 3872.

4. Паспорт национального проекта «Национальная программа «Цифровая экономика Российской Федерации»» (утв. президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 04.06.2019 № 7). – URL: https://digital.gov.ru (дата обращения: 10.03.2022).

5. Об утверждении Доктрины информационной безопасности Российской Федерации: указ Президента Российской Федерации от 05.12.2016 № 646 // Собр. законодательства Рос. Федерации. – 2016. – № 50, ст. 7074.

II. Учебная, научная литература и иные материалы

1. Аносов А. В. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: учебное пособие: в 2 ч. М.: Академия управления МВД России, 2019. Ч. 1.

2. Антонян Ю. М. Мотивация преступного поведения: монография. М.: Издательство: Юрлитинформ, 2018.

3. Атаманов Р. С. Основы методики расследования мошенничества в сети Интернет: дис. ... канд. юрид. наук. М., 2012.

4. Баландюк Р. О. Методика расследования отдельных видов преступлений, совершаемых в сфере интернет-технологий / Р. О. Баландюк [и др.] // Вестник Белгородского юридического института МВД России. 2015. № 1. С. 71.

5. Батурин Ю. М. Компьютерные правонарушения: криминализация, квалификация, раскрытие / Ю. М. Батурин, А. М. Жодзишский // Советское государство и право. 1990. № 12. С. 88.

6. Батурин Ю. М. Проблемы компьютерного права. М., 2018.

7. Гаврилин Ю. В. Особенности криминалистической характеристики неправомерного доступа к компьютерной информации // Известия Тульского государственного университета. Сер.: Современные проблемы законодательства России, юридических наук и правоохранительной деятельности. 2020. Вып. 1. С. 195.

8. Гаврилин Ю. В. Расследование неправомерного доступа к компьютерной информации. М., 2020.

9. Гаврилин Ю. В. Расследование неправомерного доступа к компьютерной информации: дис. ... канд. юрид. Наук. М., 2000.

10. Григоренко С. В., Ткаченко С. Н., Каспаров А. А. Преступления в сфере компьютерной информации. М., 2019.

11. Дворецкий М. Ю. Преступления в сфере компьютерной информации. Научно-практический комментарий к главе 28 Уголовного кодекса Российской Федерации. Тамбов, 2017.

12. Жертвами китайских хакеров стали пять нефтяных гигантов. – URL: https://oilcapital.ru/news/markets/11-02-2011/zhertvami-kitayskih-hakerov-stali-pyat-neftyanyh-gigantov (дата обращения: 05.03.2022).

13. Клаус Шваб: пандемия как трамплин. – URL: https://stolcom.com/klaus-shvab-pandemiya-kak-tramplin/ (дата обращения: 10.03.2022).

14. Краснова Л. Б. Компьютерные объекты в уголовном процессе и криминалистике: дис. ... канд. юрид. наук. Воронеж, 2015. С. 11.

15. Мещеряков В. А. Основы методики расследования преступлений в сфере компьютерной информации: дис. ... д-ра юрид. наук. Воронеж, 2001.

16. Осипенко А. Л. Борьба с преступлениями в глобальных компьютерных сетях: Международный опыт: Монография. М.: Норма, 2018.

17. Отчет «Digital 2022 Russian Federation» – Цифровые тенденции в России в 2022 году. Режим доступа URL: https://cpa.rip/stati/digital-2022-russian-federation/ (дата обращения: 12.01.2022).

18. Пиратское ПО в России и мире. Нелицензионное ПО. – URL: https://www.tadviser.ru/index.php (дата обращения: 03.03.2022).

19. Преступники начали выдавать «разрешения» раньше официальных властей. – URL: https://dailystorm.ru/rassledovaniya/chto-sluchitsya-esli-kupit-cifrovoy-propusk-v-telegram (дата обращения: 12.03.2022).

20. Простосердов М. А. Экономические преступления, совершаемые в киберпространстве, и меры противодействия им: дис. ... канд. юрид. наук. М., 2016.

21. Социальные сети в России: цифры и тренды, осень 2021 // Блог Brand Analytics. Режим доступа URL: https://br-analytics.ru/blog/social-media-russia-2021/ (дата обращения: 12.01.2022).

22. Троян Ginp зарабатывает на коронавирусе. – URL: https://teletype.in/@kasperskydaily/ROdekypzw (дата обращения: 12.03.2022).

23. Ущерб от компьютерного пиратства: цифры и факты. – URL: http://adobereal.ru/index.php/pravovye-aspekty/ushcherb-ot-kompyuternogo-piratstva-tsifry-i-fakty (дата обращения: 03.03.2022).

24. Хакеры выбили крупнейший в истории выкуп из корпорации, атакованной шифровальщиком. – URL: https://www.cnews.ru/news/top/2021-05-26_hakery_poluchili_rekordnyj (дата обращения: 03.03.2022).

25. Цирлов В. Л. Основы информационной безопасности автоматизированных систем. М., 2018.

26. Чуть меньше сна: сколько времени россияне сидят в интернете. Режим доступа URL: https://www.gazeta.ru/tech/2020/02/12/we_are_social.shtml (дата обращения: 12.01.2022).

27. Шевко Н. Р. Интернет-технологии против терроризма // Противодействие терроризму и экстремизму в информационных системах: Сб. науч. ст. Всерос. конф. – М.: Московский университет МВД России имени В. Я. Кикотя, 2020.

28. Chainalysis: 55% незаконно полученных криптовалют отмываются через 5 сервисов. – URL: https://bits.media/chainalysis-55-nezakonno-poluchennykh-kriptovalyut-otmyvayutsya-cherez-pyat-servisov/ (дата обращения: 10.03.2022).

29. Global Digital 2022: вышел ежегодный отчет об интернете и социальных сетях – главные цифры. Режим доступа URL: https://www.sostav.ru/publication/we-are-social-i-hootsuite-52472.html (дата обращения: 12.01.2022).

30. Group-IB: шпионские программы лидируют в почтовых рассылках, паразитирующих на теме коронавируса. – URL: https://www.group-ib.ru/media/covid-phishing-campaings/ (дата обращения: 12.03.2022).

III. Эмпирические материалы

1. Приговор Канашского районного суда (Чувашская Республика) № 1-29/2019 от 19 марта 2019 г. – URL: https://sudact.ru/regular/doc/Sz3pRC3muCgE/ (дата обращения: 05.03.2022).

2. Портал правовой статистики Генеральной Прокуратуры Российской Федерации. – URL: http://crimestat.ru/analytics (дата обращения: 10.03.2022).

«Материал вычитан, цифры, факты, цитаты сверены с первоисточником. Материал не содержит сведений, составляющих государственную и служебную тайну». _____ А.С. Куланбаев