Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Южно-Уральский государственный университет
(национальный исследовательский университет)»
ЮРИДИЧЕСКИЙ ИНСТИТУТ
Кафедра «Правоохранительная деятельность и национальная безопасность»

ИНФОРМАЦИОННО-ТЕХНОЛОГИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ ПО РАССЛЕДОВАНИЮ ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

ФГАОУ ВО «ЮУрГУ» (НИУ) – 40.05.02. 2016. 517. ВКР

Руководитель работы,
д-р. юрид. наук, доцент
заведующий кафедрой
Сергей Васильевич Зуев
_____2021 г.

Автор работы,
студент группы Ю-517
Владимир Анатольевич Гайдук
_____2021 г.

Нормоконтролер,
Вера Александровна Задорожная
_____2021 г.

Челябинск
2021

АННОТАЦИЯ

Гайдук В.А. Выпускная квалификационная работа «Информационно-технологическое обеспечение деятельности органов внутренних дел по расследованию преступлений в сфере информационных технологий»: ФГАОУ ВО «ЮУрГУ» (НИУ), Ю-517, 92 с., библиогр. список – 75 наим.

Объектом выпускной квалификационной работы выступают общественные отношения, связанные с информатизацией общества и использованием информационных технологий в деятельности ОВД.

Предметом исследования являются нормативные правовые акты, регламентирующие деятельность ОВД в сфере информационных технологий, специфика применения информационных технологий ОВД, задачи ОВД в данной сфере и методы их решения, возникающие в связи с этим проблемы и пути их преодоления.

Цель выпускной квалификационной работы состоит в исследовании преступлений в сфере информационных технологий,особенностей информационно-технологического обеспечения деятельности ОВД, выявлении возникающих в связи с этим проблем и способов их преодоления, а также в определении специфики и направлении деятельности ОВД по борьбе с преступлениями в сфере информационных технологий.

В работе рассматривается понятие информации, её роль и влияние на современное общество, исследуются преступления в сфере информационных технологий и методы ОВД по борьбе с ними и устранении препятствий при осуществлении данной деятельности ОВД.

Результаты исследования могут быть полезны при изучении учебных дисциплин «Оперативно-розыскная деятельность», «Информационные технологии в деятельности органов внутренних дел».

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

С момента зарождения человеческого общества люди испытывают потребность в общении друг с другом. по мере появления различных достижений науки и техники многие из них принимались на вооружение преступного мира. Компьютерные махинации, как правило, остаются незамеченными на фоне уличной преступности. Опасность подобного рода деяний определяется еще и тем, что компьютер постепенно во всем мире заполняет все сферы жизнедеятельности человека, что позволяет преступникам значительно расширить свою экспансию. Это означает, что преступное вторжение через ЭВТ может быть произведено в сферу космической и оборонной индустрии, политики и международных отношений и т.п.

В деятельности правоохранительных органов по противодействию преступлениям в сфере информационных технологий можно выделить ряд проблем, некоторые из них связаны с самой правоохранительной системой, другие обусловлены противодействием со стороны преступников в информационной сфере.

Органы внутренних дел уделяют особое внимание сохранности секретных сведений и выработке у сотрудников большей бдительности. Однако некоторые сотрудники недооценивают тяжесть последствий от утечки тайных сведений. Такие сотрудники проявляют недобросовестное отношение и халатность при работе с тайными документами, из-за чего тайные сведения могут быть разглашены, а также утеряны секретные предметы и документы. При этом некоторые сотрудники поддерживают сомнительные связи, и неформально разглашают важные сведения о способах и методах работы органов внутренних дел. Низкие профессиональные качества таких сотрудников, как правило, приводят к нарушению конспирации проводимых мероприятий.

Следующая проблема связана с технологическим консерватизмом информационного обеспечения правоохранительной деятельности по сравнению с динамичными и изменчивыми информационными процессами. Из практики деятельности ОВД последнего десятилетия, существующие структуры информационно-технологического обеспечения неизбежно устаревают, при этом отмечается нарастание скорости старения. Из этого можно сделать очевидный вывод, что технологические преобразования должны быть адаптивны меняющимся целям и задачам ОВД.

Также следует отдельно выделить проблему латентности и скрытности преступлений в сфере информационных технологий. Вероятность, что злоумышленник останется безнаказанным, крайне высока, это провоцирует активную миграцию преступников в данную сферу.

Цели и задачи исследования.

Основными целями исследования являются:

1. выявление детерминирующих факторов (причин и условий), а также количественных и качественных параметров преступности в сфере информационных технологий;
2. разработка научно обоснованных рекомендаций по совершенствованию деятельности правоохранительных органов по расследованию преступлений в сфере информационных технологий и мерах по их профилактике.
3. постановка указанных целей определила формулирование и содержание задач настоящего исследования:
4. дать комплексную уголовно-правовую и криминологическую характеристику преступлений в сфере информационных технологий;
5. сформулировать предложения и рекомендации по совершенствованию деятельности правоохранительных органов по расследованию преступлений в сфере информационных технологий и мерах по их профилактике.

Практическая значимость исследования состоит в том, что выводы, предложения и рекомендации, содержащиеся в нем, могут быть использованы в целях повышения эффективности профилактики преступлений в сфере информационных технологий за счет совершенствования деятельности правоохранительных органов в данной сфере.

Структура выпускного квалификационного исследования обусловлена целью и задачами исследования, содержанием и взаимосвязью исследуемых в работе проблем и логикой их рассмотрения. Выпускное квалификационное исследование состоит из введения, двух глав, заключения и списка использованной литературы.

В первой главе рассматриваются преступления в сфере информационных технологий, проводится ретроспективный, сравнительно-правовой анализ данных преступлений в уголовном законодательстве России и зарубежных стран. Проводится уголовно-правовая характеристика преступлений в сфере информационных технологий.

Во второй главе проведен анализ информационной безопасности ОВД, деятельности правоохранительных органов по расследованию преступлений в сфере информационных технологий.

В заключение на основе выводов по результатам исследования приводятся рекомендации по преодолению выявленных проблем и совершенствованию деятельности правоохранительных органов в сфере информационных технологий.

1 ПРЕСТУПЛЕНИЯ В СФЕРЕ ИФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

1.1 Понятие и классификация преступлений в сфере информационных технологий

Слово «информация» происходит от латинского information, что в переводе означает сведение, разъяснение, ознакомление. Понятие информации рассматривалось ещё в античной философии. До начала промышленной революции, раскрытие сути информации, по большей части, оставалось прерогативой философов. Во второй половине XX века вопросами теории информации стали заниматься кибернетика и информатика.

«Информация это такая категория, которая отличается новизной, а также свойством устраняющим энтропию, т.е. неопределённость. Информация ценна в своём количестве и объёме, в разнице того, что было до получения информации и после»[1].

«Информационно-коммуникационные технологии (ИТ) являются одним из наиболее важных факторов, влияющих на формирование общества двадцать первого века. Их революционное воздействие касается образа жизни людей, их образования и работы, а также взаимодействия правительства и гражданского общества. ИТ быстро становятся жизненно важным стимулом развития мировой экономики. Они также дают возможность частным лицам, фирмам и сообществам, занимающимся предпринимательской деятельностью, более эффективно и творчески решать экономические и социальные проблемы. Перед всеми нами открываются огромные возможности»[2].

На данный момент не существует единого определения информации как научного термина. Поэтому существует необходимость сформулировать

[1] Зуев С.В. Информация как межотраслевая правовая категория. 1-я видеолекция // [Электронный ресурс]. URL:http://www.iuaj.net/node/2636/(дата обращения 19.05.2021).
[2]Окинавская Хартия глобального информационного общества// Дипломатический вестник. 2000. №8. С. 52.

понятие информации, которое бы применялось в уголовно-правовых исследованиях и стало средством для анализа состава информационных преступлений в УК РФ.

Компьютерная информация является одним из наиболее востребованных видов информации, это обусловлено развитием информационного общества. В отечественном уголовном праве термин компьютерная информация трактуется как любая информация, которая содержится на электронном материальном носителе. В зарубежном законодательстве используется термин «данные» вместо термина «компьютерная информация». Данные определяются как набор символов,интерпретируя которые можно получить информацию.

«В российском уголовном законе компьютерная информация понимается как сведения, представленные в форме электрических сигналов, независимо от средств их хранения, передачи и обработки»[1].

«По содержанию любая информация относится к семантической (в переводе с латинского - содержащей смысл) и к информации о признаках объекта (признаковой). Сущность семантической информации не зависит от характеристик носителя. Семантическая информация - продукт абстрактного мышления человека, отображаемые с помощью символов (сообщений) на языках общения людей объекты, явления, образы и модели. Языки общения включают как естественные языки национального общения, так искусственные профессиональные языки. Профессиональные языки создаются специалистами для экономного и компактного отображения информации. Существует множество профессиональных языков: математики, музыки, радиоэлектроники, автодорожного движения, химии и т.д. Любая предметная область содержит характерные для нее понятия и условные обозначения, часто непонятные необученному этому языку человеку»[2].

[1]Колин К.К. Информационная глобализация общества и гуманитарная революция / Alma mater (Вестник высшей школы). 2002. №8. С. 34.
[2]Кемпф В.А. Основы информационной безопасности органов внутренних дел: учеб. пособие / Барнаул : Барнаульский юридический институт МВД России, 2014. С. 36.

Перейдём к раскрытию понятия информационных преступлений. Научно-техническое развитие повлекло за собой социальные изменения, важнейшим из которых является появление информационных общественных отношений. Информация стала предметом и продуктом деятельности современного общества. Следом появился новый вид преступности – преступления в сфере информационных технологий или киберпреступность.

Информационные преступления, как разновидность преступлений, закреплены в различных главах УК, из этого родилось понятие информационного преступления и его классификация.

«Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов»[1].

Информационные преступления – это преступления, совершаемыми физическими лицами с использованием информационных технологий для достижения корыстных целей. Также в соответствии с уголовным законодательством РФ даётся следующее определение, преступления в сфере компьютерной информации - деяния, совершаемые в сфере информационных процессов и посягающие на информационную безопасность, предметом которых являются компьютерные средства и информация.Данная группа преступных посягательств является институтом особенной части уголовного законодательства, за их совершение предусмотрена ответственность главой 28 УК РФ. Относится к субинституту «Преступления против общественной безопасности и общественного порядка». Видовым объектом данных преступлений выступают общественные отношения, связанные с безопасностью информации и систем обработки информации с помощью ЭВМ.

[1]Федеральный закон Российской Федерации «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года № 149-ФЗ// СЗ РФ. 2006. № 31. Ст. 3448.

Согласно УК РФ к преступлениям в сфере компьютерной информации относятся:

1. (ст. 272 УК РФ) неправомерный доступ к компьютерной информации;
2. (ст. 273 УК РФ) создание, использование и распространение вредоносных компьютерных программ;
3. (ст. 274 УК РФ) нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей;
4. (ст. 274.1 УК РФ) неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации.

Общественная опасность данных противоправных действий заключается в том, что они могут привести к нарушению деятельности автоматизированных систем управления и контроля различных объектов, нарушению работы ЭВМ, уничтожению, модификации, искажению, копированию информации и информационных ресурсов, а также иные формы незаконного вмешательства в информационные системы, что может привести к существенному имущественному ущербу.

Неправомерный доступ к компьютерной информации (ст. 272 УК РФ), создание, использование и распространение вредоносных программ (ст. 273 УК РФ), а также неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ) совершаются только путём действий. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ) как путём действий, так и бездействием.

Создание либо использование вредоносных программ для ЭВМ преступления с формальным составом. Неправомерный доступ к компьютерной информации, нарушение установленных правил эксплуатации ЭВМ, системы ЭВМ или их сети, а также неправомерное воздействие на

критическую информационную инфраструктуру РФ преступления с материальным составом.

Виды ответственности за преступления в сфере информационных технологий. Ситуация, сложившаяся в сфере информационных технологий, потребовала принятия норм уголовного права, которые предусматривали бы ответственность за совершение преступлений в сфере компьютерной информации.

Статья 272 защищает компьютерную информацию любых предприятий, организаций, учреждений и частных лиц. Диспозиция данной нормы заключается в неправомерном доступе к охраняемой законом компьютерной информации.

Неправомерным является доступ, который противоречит действующим правовым нормам, приказам, распоряжениям и актам, регулирующим отношения по доступу группы лиц к информации.

«Информация появляется на основе событий окружающего мира. События должны быть восприняты каким-то образом и проинтерпретированы, чтобы стать информацией. Поэтому информация результат воспринятых событий (данных) и команд, требуемых для интерпретации данных и связывания с ними значения»[1].

Понятие охраняемой законом компьютерной информации очень расплывчато и охватывает практически всю информацию на электронном носителе. Информация охраняется большим перечнем законодательных актов, таких как: Конституция Российской Федерации, Гражданским кодексом РФ, законами Российской Федерации «О государственной тайне», «Об информации, информатизации и защите информации», «О рекламе», «О банках и банковской деятельности». Информация обязательно является объектом охраны хотя бы одного акта.

[1]Ржавский К.В. Информационная безопасность: практическая защита информационных технологий и телекоммуникационных систем: Учебное пособие. Волгоград: Изд-во ВолГУ, 2002. С. 32.

Необходимым условием наступления уголовной ответственности по ст. 272 УК РФ является то, что неправомерный доступ должен повлечь за собой уничтожение блокирование, модификацию, копирование информации, либо нарушение работы ЭВМ, их системы или сети.

Необходимо, различать уголовное преступление и дисциплинарный проступок. Например, преступлением не будут являться действия работника, который нарушил установленный порядок пользования компьютером, не имея корыстных целей.

Диспозиция ч. 2 ст. 272 УК РФ устанавливает, что деяние, предусмотренное ч. 1, совершённое группой лиц по предварительному сговору либо организованной группой, или лицом с использованием своего служебного положения, влечёт за собой повышенную ответственность.

Субъект преступления по ст.272 УК РФ - вменяемое физическое лицо, достигшее 16-летнего возраста. С субъективной стороны преступление характеризуется наличием прямого или косвенного умысла.Преступлением не признаётся доступ к информации без намерения совершить общественно опасное деяние.Предметом преступления является компьютерная информация. Объектом – общественные отношения, связанные с безопасностью компьютерной информации. Объективная сторона – действия, направленные на неправомерный доступ к компьютерной информации.

Примером неправомерного доступа к информации может послужить случай из судебной практики, когда «Житников Д.А. получил неправомерный доступ к программному ресурсу корпорации, скопировал его и распространял нелицензионные копии программного ресурса с целью получения выгоды»[1].

Ещё одни пример из судебной практики. «В период с марта по август 2016 года Мельниченко Н.П используя телекоммуникационную сеть

[1]Приговор суда № 1-609/2017 по обвинению Житникова Д.А по ч. 2 ст. 272 УК РФ / архив Чкаловского районного суда г. Екатеринбурга // [Электронный ресурс]. URL:https://sud-praktika.ru/precedent/420329.html/ (дата обращения 19.05.2021).

«Интернет» посредством созданной им компьютерной программы осуществлял проверку данных пользователей и формировал базу пользователей для дальнейшей продажи их на указанном сайте»[1].

Статья 273 УК РФ направлена на защиту ЭВМ, информации и имущественных интересов пользователя от компьютерных «вирусов». Диспозиция ст. 273 УК РФ заключается в создании, использовании, либо распространении программ ЭВМ или внесении изменений в существующие, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети. Состав данного преступления является формальным.

«Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными. Которые включают сбор, запись, систематизацию, накопление, хранение, изменение, извлечение, использование, передачу, обезличивание, блокирование, удаление или уничтожение персональных данных»[2].

Уничтожение информации понимается как лишение сведений, данных и информации соответствующей материальной формы. Преступлением будет являться действие, повлекшее уничтожение информации на одном носителе, даже если она имеется на другом.

Блокирование информации - это лишение возможности правомерного пользователя реализовать информацию по назначению.Полагается, что ответственность наступает лишь при несанкционированном наступлении негативных последствий, так как уничтожение и блокирование иногда проводятся и в разрешительном порядке.

---

[1] Приговор суда № 1-613/2017 по обвинению Мельниченко Н.П. по ч. 2 ст. 272 УК РФ / архив Октябрьского районного суда г. Ростова-на-Дону URL:https://sud-praktika.ru/precedent/467627.html / (дата обращения 19.05.2021).

[2]Федеральный закон «О персональных данных» от 27 июля 2006 г. №152-ФЗ // Российская газета. 2006. № 4131.

Предметом данного преступления является компьютерная информация или компьютерное оборудование. Объект – общественные отношения, связанные с безопасностью информации. Объективная сторона выражена действием, направленным на создание, использование и распространение вирусных программ.

Субъект преступления – вменяемое физическое лицо, достигшее 16-летнего возраста. Субъективная сторона выражена прямым умыслом. Во второй части ст. 273 УК РФ предусмотрена ответственность за те же деяния, которые повлекли за собой по неосторожности тяжкие последствия.

Существует пример из судебной практики г. Новосибирска по ст. 273 УК РФ «Семёнов Е.В. создал и распространил компьютерную программу, заведомо предназначенную для несанкционированной модификации компьютерной информации. Был оправдан в связи с деятельным раскаянием»[1].

Как пример, «тяжкими могут быть признаны последствия в случае причинения особо крупного материального ущерба, аварий, искажений информации, составляющей государственную тайну»[2].

Ст. 274 УК РФ предусматривает ответственность за нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим к ним доступ, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации. Условием её наступления является причинение деянием существенного вреда.

Объективная сторона - прямой умысел. Ответственность по ч.2 ст.274 УК РФ наступает в случае причинения тем же деянием по неосторожности тяжких последствий.

---

[1]Приговор суда № 1-926/2017 по обвинению Семёнова Е.В. по ч. 1 ст. 273 УК РФ / архив Ленинский районный суд г. НовосибирскаURL: https://sud-praktika.ru/precedent/456303.html/ (дата обращения 19.05.2021).

[2]Закон РФ «О государственной тайне» от 21 июля 1993 г. № 5485-I // Российская газета. 2010. № 262.

«Введение уголовной ответственности за компьютерные преступления необходимо, однако этого недостаточно для эффективной борьбы с ним. Существенным шагом стало бы создание специальных подразделений по борьбе с компьютерными преступлениями, в том числе с хищениями, совершаемыми путём несанкционированного доступа в компьютерные сети и базы данных»[1].

«Классификация компьютерных преступлений. К основным видам компьютерных преступлений относятся:

1. онлайн-мошенничество;
2. клевета, оскорбления и экстремистские действия в Сети;
3. DoS – атаки;
4. дефейс;
5. вредоносные программы»[2].

Онлайн-мошенничество на практике осуществляется следующими способами:

1. фиктивные интернет-магазины;
2. Рассылка по сайтам о ложных уязвимостях в платёжных системах;
3. Мошеннические сайты и рассылки, предлагающие удалённую работу.

Ст. 497 ГК РФ предусматривает, что договор розничной купли-продажи может быть заключен на основании ознакомления покупателя с предложенным продавцом описанием товара посредством каталогов, проспектов, буклетов, фотоснимков, средств связи или иными способами, исключающими возможность непосредственного ознакомления потребителя с товаром либо образцом товара при заключении такого договора. Это даёт множество возможностей для мошенничества.

---

[1]Абромович А.М. Диалектика правовой информатизации/ А.М. Абромович - заместитель Главы Администрации Президента Республики Беларусь, д.ю.н., профессор // Современные компьютерные технологии в системах правовой информации: тез. докл. конф., г. Минск, 21-22 нояб. 2002 г. [Электронный ресурс] URL: http://ncpi.gov.by/Conf/tezis.asp? 3/ (дата обращения 19.05.2021).

[2]Бугроменко В.Н. TERRA SOCIUM / Социс. 1992. №11. С. 70.

Клевета, оскорбления и экстремистские действия в Сети. Суть преступного деяния заключается в размещении оскорбительных, экстремистских материалов в сети интернет.

«При разрешении дел, связанных с деятельностью средств массовой информации, необходимо принимать во внимание, что осуществление свободы выражения мнений и свободы массовой информации налагает особые обязанности, особую ответственность и может быть сопряжено с ограничениями, установленными законом и необходимыми в демократическом обществе для уважения прав и репутации других лиц, охраны государственной безопасности и общественного порядка, предотвращения беспорядков и преступлений, охраны здоровья и нравственности, предотвращения разглашения информации, полученной конфиденциально, обеспечения авторитета и беспристрастности правосудия»[1].

Предметом преступного посягательства выступают честь, достоинство личности, деловая репутация, национальные и религиозные чувства. В редких случаях целью такого деяния может быть провокация ложного обвинения другого лица в клевете, оскорблениях, экстремизме.

Состав преступления устанавливается в процессе проведения экспертной оценки. До результатов экспертизы распространение материала защищено конституционным правом на свободу слова.

Если информация размещается правонарушителем самостоятельно с использованием автоматизации, остаются следы поиска, настройки и пробные запуски программы. Когда информация размещается через профессионалов, искать следы необходимо через объявления, в переписках и телефонных разговорах с ними. Также правонарушитель будет

[1]Постановление Пленума Верховного Суда Российской Федерации «О практике применения судами Закона Российской Федерации «О средствах массовой информации»» от 15 июня 2010 г. № 16// Российская газета. 2010. №132.

просматривать размещённые им материалы, вследствие чего останутся соответствующие следы.

«DoS- атаки. Один из видов неправомерного доступа, который приводит к блокированию информации и нарушению работы ЭВМ с использованием уязвимостей в атакуемой среде, либо без использования таковых»[1].При подготовке и совершении DoS – атаки образуются следующие следы:

1. инструментарий атаки, то есть программные средства, установленные на компьютере злоумышленника или на сторонних компьютерах, используемых в данных целях;
2. следы поиска, тестирования и приобретения программных средств;
3. статистика трафика операторов связи, через сети которых проходила атака;
4. журналы технических средств защиты – детекторов атак и аномалий трафика, специализированных фильтров и систем обнаружения вторжений;
5. следы от изучения подозреваемым лицом рекламы исполнителей атак, их переговоров и денежных расчётов;
6. следы от обращений подозреваемого к атакуемому ресурсу в период атаки, с целью контроля её действенности.

«Дефейс. Преступление заключается в том, что злоумышленник разными приёмами и способами изменяет внешний вид веб-сайта потерпевшего»[2].

На взломанном компьютере остаётся мало следов, злоумышленник старается уничтожить их. Найти больше следов можно на компьютерах, которые хакер использует в качестве промежуточных узлов для доступа к

[1]Мазуров В.А. Компьютерные преступления: классификация и способы противодействия. М., 2002. С.21.
[2]Куприянова Г.И. Информационные ресурсы INTERNET / М.: ИПК госслужбы, 1998. С. 56.

атакуемому сайту. На собственном компьютере злоумышленника можно найти следы переработанной или новой страницы сайта, средства для осуществления несанкционированного доступа, средства для поиска уязвимостей на сайте.

Также хакеру необходимо привлечь общественное внимание к дефейсу. Соответственно, злоумышленник сразу после взлома или немного ранее оповестит мир о своём преступлении. Это могут быть объявления на различных форумах или сообщения по электронной почте. Все эти действия оставят дополнительные следы.

Вредоносные программы. Основные их разновидности:

1. троянские программы, снабжённые механизмом самораспространения;
2. программы для похищения персональных данных, которые после используются для мошенничества или хищения;
3. вредоносные программы скрытно внедряющиеся на персональный компьютер и показывающие пользователю рекламу;
4. логические «бомбы», которые автоматически уничтожают всю чувствительную информацию через определенное время илипри выполнении какого-либо условия;
5. троянские программы, скрытно внедряющиеся на компьютер жертвы, затем шифрующие файлы хранящие пользовательскую информацию, после чего они предъявляют требование о выкупе за возможность восстановления файлов пользователя.

При изготовлении вредоносных программ можно обнаружить следующие цифровые следы:

1. исходный текст вредоносных программ;
2. программные средства для управления вредоносными программами;
3. следы тестирования вирусов под различными вариантами ОС.

«Информационное общество – это общество, в котором формообразующую роль играет информация, выступающая в качестве стратегического ресурса, а основной ценностью является экономия времени за счет использования информационных технологий. В основе такого общества лежит представление об информации как основном предмете человеческого труда: сегодня успешными странами являются не те, которые обладают большой территорией, огромным количеством природных ресурсов или высокой степенью индустриализации общества. В современном мире развитыми странами считаются те, которые обладают наиболее ценным капиталом – людьми, способными преобразовывать ресурсы во все более и более сложные формы информации: поисковые системы, компьютерные программы, новейшие цифровые устройства. Развитые государства могут обладать минимумом природных ресурсов, при этом являясь мощнейшими экономиками мира (как, например, Сингапур или Япония). В высшей степени востребован и высшую степень ценности имеет не просто продукт, а информационный, цифровой продукт»[1].

«С развитием цифрового общества всё более широкое распространение получают преступления в сфере информационных технологий. Данная категория преступлений объединяется новым термином «киберпреступность»»[2]. Этот термин появился ещё в 60-ых годах прошлого столетия, сейчас получил широкое распространение в русском языке, однако всё ещё не укрепился в российском законодательстве. Одной из причин недостаточной эффективности противодействия киберпреступности я вижу консерватизм системы правоохранительных органов. Киберпреступность развивается синхронно с совершенствованием технологий, и безнаказанно действует, пока разрабатывается законодательство.

[1]Основы теории электронных доказательств: монография / под ред. докт. юрид. наук С.В. Зуева. М., 2019. С. 10.

[2] Белоглазов Е.Г., Борзунов К.К.« Применение информационных технологий в аналитической разведке». Московский Университет МВД России, 2005. С. 29.

1.2 История,современное состояние и перспективы развития преступлений в сфере информационных технологий

«Противостояние киберпреступности и закона можно представить, как эволюционный процесс. Преступники стремятся обойти законы и препятствия в своих корыстных целях, напротив правоохранительные органы стараются опередить развитие киберпреступлений и создают методы препятствующие этому. Для победы каждая из сторон поочерёдно развивается, учитывая созданные методы работы другой»[1].

«Стремление киберпреступников направлено на информацию, в том числе персональные данные, с целью извлечения выгоды, либо как способ заявить о своих профессиональных навыках»[2]. Для защиты сведений и информации правоохранительные органы разрабатывают методы информационной безопасности, отталкиваясь от объектов на которые направлены преступные посягательства. История развития информационной безопасности делится на несколько этапов.

На первом этапе ещё до 1816 года использовались естественно возникшие средства информационных коммуникаций. В этот период информационная безопасность ставила своей задачей защиту сведений о событиях, имуществе, местонахождении имеющих непосредственно для человека, которому они принадлежат жизненно важное значение.

Второй этап, начиная с 1816 года, связан с развитием и использованием искусственно создаваемых технических средств радиосвязи. С целью обеспечения скрытности и защиты радиосвязи от помех необходимо было использовать опыт первого этапа информационной безопасности, но на более высоком технологическом уровне, а именно применять помехоустойчивое кодирование сигнала и последующее декодирование принятого сигнала.

---

[1]Антопольский А.А. Правовое регулирование информационных объектов. Проблемы информатизации. М., 1999. С. 97.

[2]Гринберг Е.А. «Преступления против общественной безопасности» Свердловск, 1974. С. 84.

Третий этап, начиная с 1935 года, связан с появлением гидроакустических и радиолокационных средств. Основным методом обеспечения информационной безопасности в данный период было использование организационных и технических мер, которые были направлены на повышение защищённости радиолокационных средств от воздействия на их приёмные устройства маскирующими и имитирующими радиоэлектронными помехами.

Четвёртый этап, начиная с 1946 года, связан с изобретением и внедрением в практическую деятельность ЭВМ. «Решение задач информационной безопасности достигалось методом ограничения физического доступа к оборудованию средств добывания, переработки и передачи информации»[1].

Пятый этап, начиная с 1965 года, был обусловлен созданием и развитием локальных информационно-коммуникационных сетей. В этот период задачи информационной безопасности всё ещё решались методом физического ограничения доступа к средствам добывания, переработки и передачи информации. Локальные сети, путём администрирования и управления доступом к сетевым ресурсам, были ограничены в доступе сторонних лиц.

Шестой этап, начиная с 1973 года, стали использоваться сверхмобильные коммуникационные устройства с широким спектром задач. Угрозы информационной безопасности стали более серьёзными. Появились образования людей – хакеров, ставящих своей целью нанесение ущерба информационной безопасности частных пользователей, организаций и даже целых стран. Информация стала важнейшим ресурсом государства, а его безопасность обязательной составляющей национальной безопасности. На

[1]Бачило И.Л. Информационное право: учебник для вузов по направлению подготовки «юриспруденция» специальностям «юриспруденция» и «правоохранительная деятельность» / И.Л. Бачило, В.Н. Лопатин, М.А. Федотов; Министерства науки и образования РФ. СПб., 2005. С. 45.

этом этапе начинает формироваться информационное право – новая отрасль международной правовой системы.

Седьмой этап, начиная с 1985 года, связан с созданием и развитием глобальных информационно-коммуникационных сетей, обеспечиваемых космическими спутниками. Началось использование коммуникационных устройств с широким спектром задач и глобальным охватом в пространстве, что обеспечивалось космическими информационно – коммуникационными системами.

«Широкие возможности новейших информационных технологий могут, безусловно, свидетельствовать об их использовании в качестве достаточно эффективного и в то же время весьма доступного средства для совершения иных умышленных преступлений, предметом посягательства которых является информация, содержащаяся на машинном носителе, в ЭВМ, системе ЭВМ или их сети. К числу таких преступлений уже сегодня можно смело отнести нарушение неприкосновенности частной жизни (ст. 137 УК РФ), нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (ст. 138 УК РФ), нарушение авторских и смежных прав (ст. 146 УК РФ), разглашение тайны усыновления (удочерения) (ст. 155 УК РФ), незаконные получение и разглашение сведений, составляющих коммерческую или банковскую тайну (ст. 183 УК РФ), незаконный экспорт технологий, научно-технической информации и услуг, используемых при создании оружия массового поражения, вооружения и военной техники (ст. 189 УК РФ), государственную измену (ст. 275 УК РФ), шпионаж (ст. 276 УК РФ), разглашение государственной тайны (ст. 283 УК РФ) и преступления в сфере компьютерной информации (гл. 28 ст. ст. 272-274 УК РФ)»[1].

[1]Макаров В.А. Концептуальные основы обеспечения безопасности информации на объектах органов внутренних дел Российской Федерации учеб. пособие / Домодедово : ВИПК МВД России, 2014. С. 34.

«Для обеспечения информационной безопасности на данный момент необходимо создание макросистемы информационной безопасности человечества под эгидой ведущих международных форумов»[1].

Уровень борьбы с киберпреступлениями в России пока не соответствует ее масштабам, считают в Генпрокуратуре. В 2019 году в правоохранительные органы поступило порядка 350 тыс. сообщений о таких преступлениях, из них 80% от граждан. "В подавляющем большинстве случаев информация о противоправных посягательствах поступает в правоохранительные органы от самих потерпевших, то есть уже после совершения преступлений", - отмечают в Генпрокуратуре. Самими правоохранительными органами в 2019 году было выявлено 9 тыс. таких преступлений.

При этом у российских правоохранительных органов есть примеры успешных расследований сложных киберпреступлений, отметили в Генпрокуратуре. Например, изобличение пользователя анонимной сети TOR под псевдонимом Krokus, распространявшего детскую порнографию, когда был проведен большой объем поисково-аналитических мероприятий на сервисах «фотохостинга» и в социальных сетях и уникальное криминалистическое исследование.

«Но, несмотря на значительный рост числа уголовных дел в 2019 году (248 тыс., на 60% больше, чем в 2018 году), расследование более 70% из них приостановлено чаще всего из-за невозможности установить лиц, подлежащих привлечению в ответственности»[2].

Несмотря на то, что среди IT-преступлений хакерские преступления (неправомерный доступ к компьютерной информации, создание и оборот вредоносных программ) составляет около 1%, в Генпрокуратуре считают

[1]Голубков, А. Концепция формирования и развития единого информационного пространства России и соответствующих информационных ресурсов / Вестник Российского общества информатики и вычислительной техники: научно-информативный журнал / ВИМИ. 1995. №4. С. 35.

[2] Общество Тасс // [Электронный ресурс]. URL: //tass.ru/obschestvo/9032391/ (дата обращения 17.05.2021)

справедливым мнение ряда ведомств о том, что санкции за хакерские преступления в России чрезмерно мягкие.

«В течение последних двух лет за совершение таких преступлений перед судом предстало чуть менее 500 человек, при этом большая часть из них получили условные сроки лишения свободы, в отношении многих уголовные дела были прекращены с назначением судебного штрафа», - отмечают в Генпрокуратуре.

За 2019-2020 годы в России зарегистрировано почти 5 тыс. таких преступлений, предусмотренных главой 28 УК РФ, львиную долю составили преступления по ст. 272 УК РФ (Неправомерный доступ к компьютерной информации). В Генпрокуратуре поддержали мнение о том, что санкции за такие преступления не соответствуют уровню общественной опасности и возможным последствиям.

Борьбе с киберпреступлениями препятствует и неопределенность в правовом статусе криптовалюты. Так, в июле 2020 года Петроградский районный суд Санкт-Петербурга, вынося приговор по делу злоумышленников, которые под видом сотрудников ФСБ принудили предпринимателя перечислить им 5 млн рублей, 99 биткойнов и более мелкие суммы в криптовалюте на общую сумму 50 млн рублей, признал, что потерпевший перевел цифровые средства под действием угроз, но не посчитал это материальным ущербом, ссылаясь на отсутствие правового статуса криптовалюты. Это решение было обжаловано прокурором.

При этом в мае 2018 года в решении по другому делу арбитражный суд фактически разрешил взыскание криптовалюты с должников, а в 2019 году Верховный суд России признал, что взятка в криптовалюте может считаться преступлением. Поэтому, по мнению Генпрокуратуры, требуется скорейшая выработка единых подходов к регулированию оборота цифровой валюты на законодательном уровне.

Простор для киберпреступлений, по оценке Генпрокуратуры, создает и неограниченный оборот sim-карт. «Случаи приобретения в одни руки, чаще

всего по чужим документам, неограниченного числа мобильных телефонных номеров не только не пресечены, но и получают все большее распространение. В результате злоумышленники остаются анонимными и безнаказанными», - отметили в Генпрокуратуре. Там назвали крайне важным усилить механизмы взаимодействия с операторами сотовой связи, чтобы контроль рынка оборота sim-карт был более прозрачен для выявления мошеннических действий, в том числе и самими операторами.

В России в 2020 году зарегистрировано 510,4 тыс. преступлений, совершённых с использованием информационно-телекоммуникационных технологий. Это на 73,4% больше, чем в предыдущем году. 80% из них (410,5 тыс.) совершены путём кражи или мошенничества.

В 2020-м злоумышленники при совершении преступлений чаще использовали банковские карты, интернет и телефон. В частности, за год количество деяний с применением пластиковых карт увеличилось на 453,1%, достигнув 190,2 тыс.

«С помощью сети интернет совершено 300,3 тыс. преступлений (+91,3%), средств мобильной связи — 218,7 тыс. (+88,3%). Зачастую одно и то же преступление может совершаться с применением одного или двух приведённых методов, уточнили в ведомстве»[1].

Злоумышленники все чаще заражают жертв не одним типом вредоносного ПО, а сразу целым «букетом» троянов. Так, в ходе одной из массовых вредоносных кампаний киберпреступники доставляли на скомпрометированные компьютеры шпионское ПО LokiBot, ворующее сохраненные учетные данные из различных приложений. Помимо кражи данных, троян загружал на устройства шифровальщик Jigsaw. К слову, шифровальщики и шпионское ПО — наиболее распространенные виды

[1] Министерство внутренних дел РФ характеристика состояния преступности в Российской Федерации [Электронный ресурс] URL: https://мвд.рф/reports/item/22678184/ (дата обращения 17.05.2020).

троянов в атаках с использованием вредоносного ПО, их доли в атаках на организации во II квартале составили 39% и 34% соответственно.

Злоумышленники дорабатывают вредоносное ПО, добавляя в него новые функции. Например, вредоносное ПО Valak, ранее выполнявшее роль загрузчика для других троянов, стало полноценным «инфостилером», похищающим учетные данные и сертификаты домена. Другой пример, вредоносное ПО Sarwent. Его разработчики добавили модуль, который отвечает за предоставление удаленного доступа к зараженным узлам по протоколу RDP. Вредоносное ПО запускает на скомпрометированных узлах RDP и разрешает подключения в параметрах брандмауэра Windows. Не исключено, что полученные с помощью нового модуля доступы злоумышленники собираются продавать или сдавать в аренду другим киберпреступникам. Во II квартале мы опубликовали статью, в которой подробно рассказали о бизнесе, связанном с незаконной продажей доступов к корпоративным сетевым ресурсам.

Во II квартале доля учетных данных выросла с 15% до 30% от общего объема данных, украденных при атаках на организации. В особой цене корпоративные учетные данные сотрудников. Их злоумышленники продают в «дарквебе» или используют для дальнейших атак, например для рассылки писем с вредоносными вложениями от имени взломанных организаций. Спросом пользуются также базы учетных данных клиентов взломанных компаний.

Специалисты отмечают:

1. тенденцию роста компаний операторов-шифровальщиков и других программ-вымогателей. Их целями являются как малый, так и крупный бизнес, государственные корпорации и даже правительство. Ситуация усложняется ростом сумм выкупа и повышением сложности самих атак.
2. более частое использование в целевых атаках уязвимостей нулевого дня и, соответственно, новых неизвестных ранее эксплоитов;

3. усложнение и распространение использования ошибок человеческого фактора: социальной инженерии, ошибок конфигураций и др.;
4. распространение атак на системы Интернета вещей и в связи с этим риск взломов внутренних систем через них и усиление таких сопутствующих киберрисков, как массовые DDoS-атаки и др.

Направленные атаки являются одним из самых опасных видов озвученных рисков. Эксперты группы компаний Angara предлагают комплексный подход к защите от направленных атак. Для снижения рисков использования злоумышленниками брешей в защите необходима реализация в компании процесса управления уязвимостями.

Анализ защищенности – это непрерывный процесс, который требует как периодического сканирования систем, так и контроля за устранением обнаруженных уязвимостей, своевременной установкой программных коррекций и приведением настроек ПО и ОС в безопасное состояние. Для эффективной защиты конечных узлов – использование средств с аналитическими поведенческими механизмами защиты: Sandbox-системы, EDR-системы. Для своевременного обнаружения и изучения действий злоумышленников в сети – создание систем ложных целей. Это также отвлекает киберпреступника от реальных целей и снижает его негативную эффективность даже в случае успешного взлома периметра.

1.3 Методы защиты информации, потенциально являющейся целью противоправных посягательств

«На определённом этапе развития информационной индустрии родилось информационное общество, в котором рабочие группы занимаются производством, хранением, переработкой и реализацией информации. Работники больше занимаются творческим трудом, который направлен на развитие интеллекта и приобретение знаний. Появилось объединённое,

не разделённое национальными и государственными границами информационное сообщество»[1].

Граждане Российской федерации обладают правом на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени. Для государства обеспечение этих прав одна из важнейших целей, особенно в условиях информационного общества.

«Под средством массовой информации понимается периодическое печатное издание, сетевое издание, телеканал, радиоканал, телепрограмма, радиопрограмма, видеопрограмма, кинохроникальная программа, иная форма периодического распространения массовой информации под постоянным наименованием (названием)»[2]

«Опорой формирования информационного общества являются информационные, телекоммуникационные технологии и связь.Благодаря новым технологиям получили ход развитие и распространение глобальных информационных сетей, открывающих новые возможности международного информационного обмена. Из этого следует рост потребности в обеспечении информационной безопасности»[3].

« Доступ к информации о деятельности судов обеспечивается посредством предоставления лицам, присутствующим в открытом судебном заседании, как участникам процесса, так и лицам, не являющимся участниками процесса, представителям редакций средств массовой

[1]Антонюк Б.Д. О проблемах законодательного регулирования деятельности в сфере информационных технологий и связи/ Б.Д. Антонюк - заместитель министра информационных технологий и связи Российской Федерации. - М., 2005. [Электронный ресурс] URL: http://www.infolaw.ru/lib/2005-3-legal-regulation-problems/ (дата обращения 17.05.2021)

[2]Федеральный закон «Закон о средствах массовой информации» от 27 декабря 1991 года № 2124-1 ФЗ// Российская газета. 2007. № 213.

[3]Доктрина информационной безопасности Российской Федерации: утверждена Президентом Российской Федерации от 9 сент. 2000 г. № Пр-1895// [Электронный ресурс]. URL: https://base.garant.ru/182535/(дата обращения 17.05.2021)

информации (журналистам) права фиксировать ход судебного разбирательства»[1].

«Угроза информационной безопасности понимается, как события или действия, которые могут привести к искажению, несанкционированному использованию или разрушению информационных ресурсов управляемой системы, аппаратных и программных средств»[2].

Информационные угрозы, как правило, обусловлены:

1. естественными факторами (наводнение, пожар и др.);
2. человеческими факторами.

В свою очередь, человеческие факторы подразделяются на:

1. угрозы, носящие случайный, неумышленный характер. Угрозы, связанные с ошибками процесса подготовки, обработки и передачи информации;
2. угрозы, связанные с умышленными действиями людей. Как пример, несанкционированный доступ к автоматизированным информационным системам.

«Умышленные угрозы ставят своей целью нанести ущерб пользователям информационных систем и делятся на активные и пассивные»[3].

Пассивные угрозы нацелены на несанкционированное использование информационных ресурсов, не оказывая при этом влияния на их функционирование (как пример, прослушивание).

Активные угрозы направлены на нарушение нормального функционирования системы с помощью целенаправленного воздействия на

---

[1] Постановление Пленума Верховного Суда РФ «Об открытости и гласности судопроизводства и о доступе к информации о деятельности судов» от 13 декабря 2012 г. № 35// Российская газета. 2012. № 292.

[2] Всемирная встреча на высшем уровне по вопросам информационного общества (World Summit on the Information Society - WSIS) Всемирный Саммит по информационному обществу// [Электронный ресурс]. URL: www.humanities.edu.ru/db/ msg/47695/ (дата обращения 17.05.2021)

[3] Городов О.А. Основы информационного права России учеб. пособие / СПб.: Юридический центр Пресс, 2003. С. 17.

аппаратные, программные и информационные ресурсы. В качестве источников активных угроз могут выступать действия злоумышленников, программные вирусы и др.

Также умышленные угрозы делятся на внутренние (возникающие внутри организации) и внешние.Внутренние угрозы – угрозы безопасности информации инсайдером (исполнителем). Для организации инсайдер является внутренним субъектом по отношению к информационным ресурсам.Внешние угрозы – угрозы информационной безопасности инициатором которых является внешний по отношению к ресурсам организации субъект (злоумышленник, удалённый хакер).

«Информационная безопасность подразумевает невозможность нанесения вреда свойствам объекта безопасности, информации и информационной инфраструктуре (защищённость от угроз)»[1].

Основные задачи системы информационной безопасности:

1. выявлять и устранять угрозы безопасности ресурсам, причины и условия, которые способствуют нанесению имущественного, материального и морального ущерба его интересам;
2. создание механизма, способов и условий для быстрого реагирования на угрозы безопасности и проявлению тенденций в функционировании предприятия;
3. эффективно пресекать посягательства на ресурсы и угрозы персоналу, основываясь на правовых, инженерно-технических и организационных мерах и средствах обеспечения безопасности.
4. создавать условия для возмещения и локализации нанесённого ущерба неправомерными действиями физических лиц, уменьшение негативного влияния от последствий нарушения безопасности на предприятии или внутри организации.

«В узком смысле понятие информационной безопасности подразумевает: надёжную работу компьютера, сохранность ценных данных,

[1]Копылов В.А. Информационное право: вопросы теории и практики / М., 2003. С. 40.

защищённость информации от несанкционированного доступа и внесения изменений, сохранность тайны переписки в электронной связи»[1].

Способы и методы обеспечения информационной безопасности. Решая проблемы защиты информации в сети, необходимо определить возможные причины и условия сбоев и нарушений, которые приводят к уничтожению или несанкционированной модификации данных. К таким причинам можно отнести:

1. сбои оборудования;
2. потери информации из-за неправильной работы ПО;
3. заражение системы компьютерными вирусами;
4. ущерб, наносимый организации несанкционированным доступом, копированием, уничтожением или модификацией информации;
5. потери информации, связанные с неправильным хранением данных;
6. ошибки пользователей и обслуживающего персонала.

Способы защиты от данных нарушений можно разделить на три группы:

1. средства физической защиты электропитания, аппаратуры, кабельной системы, дисковых массивов и др.;
2. программные средства (средства контроля доступа к информации, антивирусные программы, система разграничения полномочий);
3. административные меры (обеспечение охраны помещений, разработка действий при чрезвычайных ситуациях и др.).

Однако, подобное деление условно, так как современные технологии развиваются в направлении интеграции аппаратных и программных средств защиты. В области защиты от компьютерных вирусов и контроля доступа к данным такие аппаратно-программные средства получили наибольшее распространение.

[1]Красненкова Е.В. Обеспечение информационной безопасности в Российской Федерации уголовно-правовыми средствами: дис. канд. юрид. наук: / М., 2006. С. 9.

«В настоящее время существует тенденция концентрации информации в компьютерных системах, что вынуждает всё более усиливать контроль над её сохранностью, как в частных, так и в правительственных организациях»[1].

В частных организациях обеспечение информационной безопасности достигается за счёт ограничения доступа к ней. «Доступ к информации, составляющей коммерческую тайну, - ознакомление определенных лиц с информацией, составляющей коммерческую тайну, с согласия ее обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации»[2]. Работа в этом направлении привела к созданию новой дисциплины: безопасность информации. Специалисты в данной области отвечают за разработку и использование системы обеспечения информационной безопасности, как физической, так и логической защиты информационных ресурсов.

Для обеспечения информационной безопасности требуется много финансовых затрат, по большей части, из-за того, что трудно просчитать грань разумной безопасности и количество ресурсов, необходимых для поддержания работоспособного состояния системы. Как пример, если локальная сеть разрабатывалась в целях совместного использования лицензионных программных средств или больших файлов общедоступной информации, то нет необходимости даже в небольших затратах на шифрование данных системы.

Сначала необходимо произвести анализ имеющихся рисков и связанных с ними потерь, и только после этого проектировать, покупать или устанавливать средства защиты информации. Также нужно учесть множество факторов (юридические аспекты, взаимоотношения в коллективе, подверженность системы сбоям, вероятный ущерб от коммерческих потерь) и собрать разную информацию с целью определить подходящий тип и

[1]Крутских А.В. Международное сотрудничество в области информационной безопасности / М., 2003. С. 85.
[2]Федеральный закон «О коммерческой тайне» от 29 июля 2004 г. № 98-ФЗ// Российская газета. 2004. № 3543.

уровень безопасности. Коммерческие организации всё чаще экспортируют критическую корпоративную информацию с закрытых внутренних систем в открытую среду, из-за чего встречаются с новыми сложными проблемами во время реализации и использования систем безопасности. Увеличивается популярность распределённых баз данных и приложений по типу «клиент-сервер» при руководстве бизнесом, вследствие чего увеличивается риск несанкционированного доступа к данным и их модификации.

«Обеспечить безопасность информации можно различными методами и средствами как организационного, так и инженерного характера. Комплекс организационных мер, программных, технических и других методов и средств обеспечения безопасности информации образует систему защиты информации. При этом следует иметь в виду, что защите подлежит информация, содержащая сведения, отнесенные к государственной тайне, и другие конфиденциальные сведения»[1]

Средства физической защиты данных. Наиболее уязвимым местом линий внешней связи является кабельная система. Данные различных исследований указывают на то, что именно из-за неё происходит более половины отказов сети. Соответственно, с самого начала проектирования надёжности кабельной системы должно уделяться особое внимание.

Наилучшим образом избавить себя от проблем, связанных с неправильной прокладкой кабеля, позволяет использование получивших широкое распространение структурированных кабельных систем (например, SYSTIMAX SCS фирмы AT&T, OPEN DECconnect компании Digital, кабельной системы корпорации ЮМ).

Программные и программно-аппаратные методы защиты.Шифрование данных долгое время использовалось различными спецслужбами и оборонными ведомствами, однако сейчас, из-за роста возможностей компьютерной техники множество коммерческих компаний и даже частных

[1]Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина - СПб: НИУ ИТМО, 2012. С. 57.

лиц стали использовать средства шифрования для обеспечения конфиденциальности данных. По большей части это финансовые службы крупных компаний, которые предъявляют особые требования к алгоритмам, используемым в процессе шифрования данных. Однако рынок коммерческой системы не требует такой строгой защиты, как правительственные и оборонные ведомства, поэтому применяются продукты другого типа, как пример PGP (PrettyGoodPrivacy).

Защита от компьютерных вирусов. По данным социологического исследования, которое было проведено компанией CreativeStrategiesResearch, из 450 опрошенных специалистов 64% претерпевали вредоносное воздействие компьютерных вирусов. На данный момент к тысячам уже известных компьютерных вирусов ежемесячно прибавляется более сотни новых. Самым распространённым методом зашиты от них, уже долгое время, являются антивирусные программы.

Антивирусные программы являются наиболее действенным способом борьбы с вирусами. Большинство продуктов представленных лидерами индустрии антивирусных программ являются комплексными и обладают похожими параметрами защиты и производительности.

Антивирусы обеспечивают защиту:

1. рабочих станций;
2. файловых серверов;
3. почтовых серверов;
4. систем документооборота;
5. работы в интернете;
6. портативных устройств.

Существуют правила, соблюдая которые пользователь сможет обеспечить защиту данных от компьютерного вируса:

1. необходимо всегда делать резервные копии важных данных. Файлы могут быть удалены троянским вирусом, зашифрованы, либо повреждены;

2. большую защиту даст использование нескольких бесплатных антивирусных программ;

3. после установки антивирусной программы, после её необходимо оптимально настроить и включить автоматическое обновление.

В последнее время, как один из перспективных подходов, всё чаще находит применение сочетания программных и аппаратных средств защиты.

Защита от несанкционированного доступа. В связи с широким распространением локальных и, в особенности, глобальных компьютерных сетей обострилась проблема защиты информации от несанкционированного доступа. Зачастую ущерб бывает нанесён не злоумышленниками, а самими пользователями, которые из-за элементарных ошибок портят и удаляют данные. Поэтому, кроме контроля доступа, для защиты информации необходимо разграничение полномочий пользователя. Обе эти задачи успешно решаются при помощи встроенных средств операционных систем.Однако и в такой системе защиты есть слабое место, так как уровень доступа и возможность входа в систему определяется паролем, существует вероятность, что его подсмотрят или подберут злоумышленники.

В последнее время для исключения возможности неавторизованного доступа в сеть всё чаще используется комбинированный метод: пароль совместно с идентификацией пользователя по персональному ключу. Такой ключ может быть представлен в виде пластиковой карты или различных устройств для идентификации личности по биометрическим данным (отпечаткам пальцев, радужной оболочке глаза и др.) Для доступа к персональному компьютеру пользователю нужно вставить карту в устройство чтения и ввести свой персональный код.

«Доступ представляет собой взаимодействие между субъектом и объектом, в результате которого производится перенос информации между ними. Два фундаментальных типа доступа: чтение – операция, результатом которой является перенос информации от объекта к субъекту; запись –

операция, результатом которой является перенос информации от субъекта к объекту»[1].

Криптографическая защита данных. Криптография (также используется термин криптология) – область знаний, изучающая тайнопись (криптография) и методы её раскрытия (криптоанализ). Криптография является разделом математики.

Цель криптографической системы заключается в шифровании осмысленного исходного текста, в результате чего получается бессмысленный для человеческого восприятия шифрованный текст (криптограмма). Получатель, которому предназначается текст, должен быть способен дешифровать эту криптограмму, и таким образом, восстановив осмысленный текст. При этом криптоаналитик должен быть неспособен раскрыть исходный текст.

Примером одного из простых алгоритмов является шифр Цезаря, который заключается в простой замене каждой буквы исходного текста третьей следующей за ним буквой алфавита (при необходимости с циклическим переносом). Например, «A» заменялась на «D», «Z» на «C» и так далее.

Все методы шифрования делятся на две группы:

1. шифры с секретным ключом (симметричная схема);
2. шифры с открытым ключом (асимметричная схема).

Суть шифров с секретным ключом заключаются в наличии некой информации (ключа), человек обладающий ключом способен как зашифровать, так и дешифровать сообщение. Шифры с открытым ключом подразумевают наличие двух ключей, закрытого для зашифровки сообщений и открытого, для расшифровки.

К основным типам шифрования относятся: шифрование данных на локальных носителях (клиентское шифрование) и определённый и

[1]Нестеров С.А. Информационная безопасность и защита информации: Учебное пособие. СПб.: Изд-во Политехн. ун-та, 2009. С. 41.

конкретный математический способ обработки информации для скрытия её смысла и содержания (криптографический алгоритм).

Основные направления применения:

1. зашифровка отдельных файлов;
2. зашифровка виртуальных дисков, отдельных разделов на жёстком диске;
3. шифрование жёстких дисков целиком.

«Электронно-цифровая подпись – это последовательность символов, получая в результате криптографического преобразования исходной информации с помощью закрытого ключа электронно-цифровой подписи, который позволяет подтверждать неизменность и целостность этой информации, а также её авторство, если использовать открытый ключ электронно-цифровой подписи и его сертификат»[1].

Благодаря цифровой подписи обеспечивается:

1. удостоверение источника файла. В зависимости от деталей в файле могут быть подписаны такие поля как автор, внесённые изменения, метка времени и др.;
2. защита от изменений файла. При малейшем намеренном или случайном изменении файла изменится хэш, следовательно, подпись станет недействительной;
3. невозможность отказаться от авторства. Создать корректную подпись, можно только зная закрытый ключ, а он известен только владельцу, соответственно владелец не может отказаться от своей подписи под файлом.

Для создания подписи документа нужно вычислить значение хэш-функции для документа, затем это значение по специальному криптоалгоритму подписывается секретным ключом принадлежащим автору документа.

[1]Федеральный закон Российской Федерации «Об электронной цифровой подписи» от 10 января 2002 года № 1-ФЗ// Российская газета. 2011. № 75.

При проверке документа на подлинность нужно с помощью открытого ключа проверить подпись, затем вычислить его хэш-значение и сравнить с подписанной контрольной суммой. В случае точногосовпадения данных значений подтверждается подлинность подписи, в противном случае, документ был изменён.

На данный момент защита информации обеспечивается законодательными актами на международном и государственном уровнях. В 1981 г. Совет Европы одобрил конвенцию по защите данных, в 1984 г. В Великобритании был принят похожий закон. В Российской Федерации нормы о защите информации содержатся законе «Об информации, информатизации и защите информации» 1995г. и законе 2002 г. «О правовой охране программ для электронных вычислительных машин и баз данных».

Данными правовыми актами установлены нормы, регулирующие отношения в области формирования и потребления информационных ресурсов, создания и использования информационных систем, информационных технологий и средств их обеспечения, а также защиты информации и защиты интересов и законных прав граждан в условиях информатизации общества.

«Согласно статье 29 Конституции Российской Федерации каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Никто не может быть принужден к выражению своих мнений и убеждений или отказу от них. Каждому гарантируется свобода мысли и слова, свобода массовой информации. Цензура запрещается»[1].

Для обеспечения информационной безопасности на федеральном уровне принимаются следующие меры:

[1]Постановление Пленума Верховного Суда Российской Федерации «О практике применения судами Закона Российской Федерации «О средствах массовой информации»» от 15 июня 2010 г. № 16// Российская газета. 2010. №132.

1. осуществляется формирование и реализация единой системы государственной политики, обеспечивающей защиту национальных интересов от угроз в информационной сфере;
2. устанавливается баланс между допустимыми ограничениями распространения информации и потребностью в её свободном обмене;
3. совершенствуется законодательство РФ в сфере обеспечения информационной безопасности;
4. координируется деятельность органов государственной власти по обеспечению информационной безопасности;
5. защищаются государственные информационные ресурсы на оборонных предприятиях и стратегических объектах;
6. развиваются отечественные телекоммуникационные и информационные структуры;
7. совершенствуется информационная структура развития новых информационных технологий;
8. средства поиска, сбора, хранения, обработки и анализа информации становятся более унифицированными;

Вопросы государственной информационной безопасности оговорены в «Концепции национальной безопасности Российской Федерации», которая была создана Указом президента РФ от 17 декабря 1997 года.

В Российской Федерации борьбой с преступлениями в сфере информационных технологий занимается Управление «К» МВД РФ и отделы «К» региональных управлений внутренних дел, входящие в состав Бюро специальных технических мероприятий МВД РФ.

1.4 Информационно-технологические средства и приёмы, используемые в противодействии расследованию

Характеристика информационно-технологических средств и приемов противодействия расследованию. Современная информационная среда создала условия не только для эффективного осуществления правоохранительной деятельности, но и предоставила возможности для совершения преступлений, а также способствовала появлению новых форм и видов противостояния деятельности правоохранительных органов в расследовании преступлений. Сейчас можно смело утверждать о том, что на вооружение преступников взяты функциональные возможности информационных технологий, которые они используют для повышения эффективности сокрытия преступной деятельности и своей личности.

«Исследование вопросов использования информационных технологий в целях противодействия расследованию преступлений позволяет сформировать теоретическую базу, основываясь на которой возможно разработать приемы и способы преодоления такого противодействия»[1]. Вопросам противодействия расследованию в криминалистической науке уделялось достаточно много внимания. Некоторые авторы отмечают, что «проблема противодействия и его преодоления только лишь набирает обороты и развитие такого института для криминалистики, как прикладной науки имеет большое практическое значение, так как фактически вся деятельность органов расследования заключается в преодолении противодействия как такого».

«Противодействие расследованию преступлений — это явление, существующее в реальной действительности (объективной реальности) после возбуждения уголовного дела и представляющее собой совокупность (комплекс, систему) умышленных противоправных действий (способов),

[1]Левин В.К. Концепция развития безопасных информационных технологий: обеспечение защиты информации в проектах информатизации России / Министерство науки РФ. М., 1992. С. 35.

иных умышленных действий (способов) и (или) умышленного противоправного и не противоправного бездействия «внутренних» и «внешних» субъектов противодействия, препятствующих в ходе предварительного расследования целям установления обстоятельств, подлежащих доказыванию, состоящему в собирании, проверке (исследовании), оценке и использовании доказательств и результатов оперативно-розыскной деятельности»[1]. В приведенном определении автор уточняет, что противодействие расследованию может существовать только после возбуждения уголовного дела. Предполагаем, что автор исходит из того, что если нет расследования, значит, и не может быть и противодействия ему. Появление противодействия расследованию с началом предварительного следствия связывают и другие авторы.

Также «существует понимание противодействия расследованию, как умышленные действия (или систему действий), направленные на воспрепятствование выполнению задач предварительного расследования и установлению объективной истины по уголовному делу, на уклонение виновного от уголовной ответственности путем воздействия на информацию о преступном деянии или на ее носителя»[2].

Вместе с тем, в научном сообществе существуют иные точки зрения относительно сущности противодействия. Есть следующее определение противодействию расследованию «совокупность умышленных противоправных и иных действий преступников (а также связанных с ними лиц), направленных на воспрепятствование деятельности правоохранительных органов по выявлению, раскрытию и расследованию преступных деяний».[3] По мнению автора, противодействие как явление, не

[1]Доронин А.И. Разведывательное и контрразведывательное обеспечение финансово-хозяйственной деятельности предприятия /Тула, 2000. С. 43.
[2]Емельянов Г. В. Информационная безопасность России. Основные понятия и определения. Учебное пособие / Под общ. ред. проф. А. А. Прохожева. М.: РАГС при Президенте РФ, 2009. С. 46.
[3]Жаров А.С. Правовые аспекты информационной безопасности: новые подходы / Национальные интересы. 2005. №2. С. 32.

связано с возбуждением уголовного дела и началом предварительного расследования. В данном определении подчеркивается, что это действия направленные в целом на воспрепятствование деятельности правоохранительных органов по решению специальных задач.

А.Ф. Волынский, в своем определении противодействия расследованию, также жестко не указывает на такую последовательность событий, как возбуждение уголовного дела, а затем противодействие. По его мнению «противодействие расследованию представляет собой систему умышленных, противоправных действий (бездействия) лиц, направленных на воспрепятствование деятельности правоохранительных органов по собиранию и использованию розыскной и доказательственной информации в процессе возбуждения и расследования уголовного дела, а в итоге - на воспрепятствование правосудию»[1].

Несмотря на схожую позицию, относительно начала существования противодействия в этих определениях есть принципиальное отличие, связанное с тем, что А.Ф. Волынский к противодействию расследованию относит исключительно противоправные умышленные действия (бездействий). С такой точкой зрения сложно согласиться, связано это с тем, что действия по сокрытию и иные действия, противодействующие расследованию, не обязательно могут носить характер противоправных. Например, умалчивание какой-либо информации, использование «анонимных» средств связи, программных средств шифрования и т.д. Разнообразие предлагаемых определений обуславливает научный интерес к рассматриваемому явлению, так в своем исследовании Л.Е. Чистова проведя анализ определений «противодействие расследованию» приходит к выводу, что «…следует различать противодействие расследованию преступлений и противодействие правоохранительным органам по их выявлению».

[1]Криминалистика: Учебник для вузов / под ред. А.Ф. Волынского. М.: Закон и право, ЮНИТИ-ДАНА, 1999. С. 85.

Действительно в научной литературе встречаются множество трактовок понятия: противодействие предварительному следствию, противодействие расследованию, противодействие деятельности правоохранительных органов и т.д. Однако зачастую авторы таких определений подчеркивают лишь возможность существования или отсутствия противодействия как такого, до стадии возбуждения уголовного дела.

Сегодня многие отмечают, что учение о противодействии расследованию динамично развивается и ему уже «тесно» в рамках периода предварительного следствия. Так, Р.С. Белкин отмечал «Если раньше под противодействием расследованию понимали преимущественно различные формы и способы сокрытия преступления, то теперь это понятие наполнилось более широким содержанием и может быть определено как умышленная деятельность с целью воспрепятствования решению задач расследования и в конечном счете установлению истины по делу»[1].

Действительно, мы считаем, что методологически оправданным исследование вопроса противодействия расследованию, будет с позиции возможности его существования до момента возбуждения уголовного дела. Во-первых, объектом криминалистики является преступная деятельность, в нее традиционно вплетена деятельность по противодействию расследованию как элемент, «…противодействие раскрытию и расследованию преступлений является элементом преступной деятельности». Криминалисты изучают преступную деятельность с функциональной стороны от подготовки к совершению преступления до его сокрытия. Вместе с тем, было бы не логично искусственно ограничивать себя в изучении такого ее элемента как противодействие расследованию только в рамках процессуального периода предварительного следствия и судебного рассмотрения.

Во-вторых, изучение функциональной стороны преступной деятельности предполагает исследование всего механизма преступления, его

[1]Криминалистика: учебник для вузов / под ред. Р.С. Белкина. М.: НОРМА, 2001. С. 46.

следов отображений, что будет являться теоретической базой для выработки научно обоснованных криминалистических рекомендаций преодоления противодействия. Не секрет, что многие возможности реализации противодействия расследованию формируются на стадии подготовки и совершения преступления, нередко задолго до акта возбуждения уголовного дела.

В-третьих, при формулировке определения противодействие расследованию, следует понимать процесс расследования не в уголовно-процессуальном, а в криминалистическом смысле как процедуру сбора информации, познания и совершения определенных действий субъектом расследования. Для криминалистики изучающей функциональные стороны преступной и правоохранительной деятельности процесс раскрытия преступления представляет собой деятельность, поделенную на этапы. При этом, временные отрезки указанных этапов жестко не соотносятся с какими-либо стадиями уголовно-процессуальных действий или процессуальных сроков расследования, они обусловлены информационной и функциональной составляющими. С позиции криминалистики «этап расследования – это ограниченный период расследования, характеризующийся особыми задачами, решаемыми в условиях специфических для данного этапа следственных ситуаций».

В ходе написания первой главы былирассмотрены понятия информации и преступлений в сфере информационных технологий, их место в Российском и зарубежном законодательстве. Была дана классификация преступлений в сфере информационных технологий и преступлений совершаемых с использованием сети «Интернет». Этот этап исследования позволяет понять и оценить степень важности информации для функционирования всех сфер государства и общества. Учитывая это можно сделать вывод о том, насколько серьёзную угрозу представляют преступления в сфере информационных технологий, в особенности на государственном и международном уровне.

Также в ходе исследования был рассмотрен вопрос об истории развития и современном состоянии информационных преступлений и методов борьбы с ними, так как эти сферы развиваются и существуют во взаимосвязи друг с другом. Оценив историю развития и современность можно спрогнозировать перспективы развития преступлений в сфере информационных технологий. Ряд учёных считают, что количество информационных преступлений со временем будет неизбежно расти.

Серьёзной проблемой является то, что развитие информационных технологий даёт возможность преступникам оказывать противодействие расследованию. По данному вопросу были рассмотрены информационно-технологические средства и приемы, используемые в противодействие расследованию. Система правоохранительных органов развивается, соответственно разрабатываются методы препятствующие противодействию расследования.

Информация является ценным ресурсом, и чем выше её ценность, тем выше вероятность, что её будут стремиться заполучить злоумышленники. Поэтому был рассмотрен вопрос об общих методах защиты информации, потенциально являющейся целью противоправных посягательств. Деятельность правоохранительных органов в сфере информационных преступлений сложный процесс, требующий большое количество ресурсов. Наиболее эффективным и в то же время наименее затратным методом предупреждения информационных преступлений будет обеспечение качественной информационной безопасности.

2 ПРОТИВОДЕЙСТВИЕ ОРГАНОВ ВНУТРЕННИХ ДЕЛ ПРЕСТУПЛЕНИЯМ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

2.1 Система обеспечения информационной безопасности органов внутренних дел

«В системе обеспечения информационной безопасности правоохранительных органов в качестве наиболее действенных и эффективных методов, направленных на предупреждение и профилактику информационных преступлений, следует выделить правовые, организационные и технические методы»[1].

К техническим методам, как правило, относят защиту от несанкционированного доступа к системам и сетям, резервирование персональных подсистем, организацию вычислительной сети с последующим распределением внутриорганизационных ресурсов при нарушении работоспособности отдельных элементов, установку оборудования пожаротушения, установку сигнализации, оснащения здания замками и охраной и др.

«К организационным методам следует отнести охрану вычислительных центров, тщательный подбор персонала, исключение ведения важной работы одним сотрудником, разработку плана восстановления полноценного функционирования вычислительного центра после поломок и сбоев, выбор наиболее защищённого местоположения центра, организацию внутренней безопасности и т. д.»[2].

«Правовые меры включают в себя разработку, а затем внедрение правовых норм, устанавливающих уголовную ответственность за преступления такого рода, защиту авторских прав программистов, усовершенствование гражданского и уголовного законодательства и

[1]Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. М.: Горячая линия Телеком, 2010. С. 37.

2 Федоров В. Компьютерные преступления: выявление, расследование и профилактика // Законность. № 6. 2004. С. 44.

судопроизводства»[1]. Также к правовым мерам следует отнести вопросы государственного контроля над разработчиками различных компьютерных программ, а также принятие международных контрактов и договорных соглашений, ограничивающих их деятельность в случае, если они оказывают влияние на социальные, экономические или военные сферы деятельности государства.

«Под объектами информационных правоотношений понимаются блага, существующие в формах информации, документированной информации и информационных систем, по поводу которых возникает и осуществляется деятельность участников этих правоотношений. При этом информация является благом особого рода, а документированная информация и информационные системы – благами материальными»[2].

«Основной целью использования информационных технологий в деятельности федеральных органов государственной власти является повышение эффективности механизмов государственного управления на основе создания общей информационно-технологической инфраструктуры, включающей государственные информационные системы и ресурсы, а также средства, обеспечивающие их функционирование, взаимодействие между собой, населением и организациями в рамках предоставления государственных услуг»[3]

В завершение отметим, что даже «использование самых современных аппаратных методов, программных методов и любых других, как правило, не может гарантировать полной и абсолютной надежности и безопасности в компьютерной сфере. Вместе с этим, свести риски потерь к минимуму,

[1]Вопросы Министерства юстиции Российской Федерации Указ Президента РФ от 13 октября 2004 г. №1313// [Электронный ресурс]. URL: www.consultant.ru/document/cons_doc_LAW_49892// (дата обращения 19.05.2021).

[2]Нестеровский О.И. Основы информационной безопасности в ОВД: методические рекомендации / Электр. дан. и прогр. Воронеж : Воронежский институт МВД России, 2015. С. 29.

[3]Концепция использования информационных технологий в деятельности федеральных органов государственной власти до 2010 года// [Электронный ресурс]. URL: https://digital.gov.ru/ru/documents/3017/ (дата обращения 12.05.2020).

возможно только при наличии комплексного правового подхода к вопросу защиты и безопасности компьютерных систем»[1].

Современный мир строится на повсеместном применении компьютерной техники, вследствие чего поменялся подход к пониманию информации. С появлением вычислительных машин информация начала восприниматься как неотъемлемая часть жизни любого человека, и взгляд на информацию сменился с восторженного на обыденный.

Государству необходимо лучше взаимодействовать с обществом, активно использующим информационные технологии. Россия развивается в данном направлении, и ставит одной из своих целей «повышение качества взаимоотношений государства и общества путем расширения возможности доступа граждан к информации о деятельности органов государственной власти, повышения оперативности предоставления государственных и муниципальных услуг, внедрения единых стандартов обслуживания населения»[2]

Почему же информации необходима обработка и, тем более, правовая защита? Информацию можно разделить на правовую и не правовую. Правовая информация делится на нормативную и ненормативную.

«Нормативная информация формируется в результате правотворческой деятельности и содержится в нормативных правовых актах. К ней относится Конституция РФ, Федеральные конституционные законы, Федеральные законы, Законодательные акты субъектов РФ, Указы Президента РФ, Постановления Правительства РФ, различные нормативные акты органов исполнительной власти всех уровней и акты органов местного самоуправления»[3].

---

[1] Лопатина Т.М. Виктимологическая профилактика преступлений в сфере компьютерной информации // Современное право. № 7. 2005. С.52.

[2]Электронная Россия (2002-2010 годы): Федеральная целевая программа// [Электронный ресурс]. URL: http:// digital.gov.ru/ru/activity/programs/6/ (дата обращения 12.05.2021)

[3]Концепция управления государственными информационными ресурсами: Рекомендована Правительством Российской Федерации для использования при разработке федеральных

Ненормативная информация формируется в результате правоохранительной и правоприменительной деятельности. Такая информация делится на несколько больших групп:

1. информация о состоянии правопорядка и законности;
2. информация о гражданско-правовых отношениях, договорных и иных обязательствах;
3. информация, отражающая административную деятельность органов исполнительной власти и местного самоуправления по исполнению нормативных предписаний;
4. информация судов и судебных органов (судебные решения и судебные дела);
5. правоохранительная информация.

«Информационная безопасность органов внутренних дел – это состояние защищённости интересов ОВД в информационной сфере в соответствии с возложенными на них задачами»[1].

К существенным элементам информационной сферы относятся:

1. ведомственная информация и информационные ресурсы;
2. ведомственная информационная инфраструктура, средства и системы информатизации;
3. сотрудники органов внутренних дел, в качестве субъектов исполнения информационной деятельности;
4. система нормативно-правового регулирования.

«Безопасность информации (данных) определяется отсутствием недопустимого риска, связанного с утечкой информации по техническим каналам, несанкционированными и непреднамеренными воздействиями на

программ по формированию общедоступных государственных информационных ресурсов// [Электронный ресурс]. URL: : http://www.elrussia.ru/166776

[1]Журавленко Н.И. Кадулин Б.Е. Основы информационной безопасности: Учебное пособие. М.: Мос УМВД России. 2012. С. 53.

данные и (или) на другие ресурсы автоматизированной информационной системы, используемые в автоматизированной системе»[1].

«Обеспечение информационной безопасности помогает защитить информацию и информационную инфраструктуру предприятия от негативных воздействий. Такие воздействия могут носить случайный или преднамеренный, внутренний или внешний характер. Результатом таких вмешательств может стать потеря важной информации, ее несанкционированное изменение или использование третьими лицами. Поэтому информационная безопасность — это важный аспект защиты бизнеса и обеспечения его непрерывности»[2].

В правоохранительной и судебной сферах к особо значимым объектам обеспечения информационной безопасности следует отнести:

1. информационные ресурсы федеральных органов исполнительной власти, реализующих правоохранительные функции и судебных органов, их информационно вычислительные центры, содержащие сведения и оперативные данные;
2. информационно вычислительные центры, их информационно, программное, техническое и правовое обеспечение;
3. информационную инфраструктуру.

Угрозы в правоохранительных и судебных сферах делятся на внутренние и внешние.

Внешние угрозы:

1. разведывательная деятельность специальных служб иностранных государств, а также международных преступных сообществ и групп, занимающихся сбором сведений о раскрытии планов деятельности,

[1]Жуйков А.А. Основы информационной безопасности в органах внутренних дел. Словарь терминов и понятий / Новороссийск : Новороссийский филиал КрУ МВД России, 2014. С. 64.

[2]Советов Б. Я. Информационные технологии : учебник для среднего профессионального образования / Б. Я. Советов, В. В. Цехановский. 7-е изд., перераб. и доп. М.: Издательство Юрайт, 2019. С. 34.

методов работы и мест дислокации специальных подразделений и органов внутренних дел;

2. деятельность иностранных государственных и частных коммерческих структур, которые стараются получить несанкционированный доступ.

Внутренние угрозы:

1. нарушение установленного регламента сбора, обработки, хранения и передачи информации, хранящейся в картотеках и автоматизированных банках данных, применяющейся при расследовании преступлений;

2. дефицит законодательного и нормативного регулирования информационного обмена в правоохранительной и судебной сферах;

3. отсутствие единой методологии сбора и обработки информации, а также хранение информации криминалистического, статистического и оперативно-розыскного направления деятельности;

4. сбои программного обеспечения в информационных системах;

5. умышленные действия, а также ошибки персонала, работающего над ведением картотек и автоматизированных банков данных.

Обеспечение безопасности информационных ресурсов и информационной инфраструктуры органов внутренних дел заключается в безопасности их наиболее важных свойств. Субъектам информационных отношений может быть причинён урон путём воздействия на процессы и средства обработки критичной для них информации, вследствие чего появляется необходимость в обеспечении защиты всей информационной системы от незаконного вторжения, хищения, уничтожения или модификации любых компонентов указанной системы в процессе её деятельности.

Безопасность каждого компонента автоматизированной системы складывается из обеспечения трёх его свойств:

1. конфиденциальности, заключающейся в возможности доступа к компоненту только тем субъектам, у которых имеются особые полномочия;
2. целостности, которая является свойством информации, отражающим способность системы противостоять несанкционированному или непроизвольному уничтожению или изменению;
3. доступности, что подразумевает возможность для субъекта, обладающего соответствующими полномочиями, в любое время получить доступ к необходимому компоненту системы.

При нарушении перечисленных свойств компонента, возникает угроза для информационной безопасности органов внутренних дел.

Следует подчеркнуть, что важнейшей целью защиты автоматизированных систем и содержащейся в них информации является предотвращение или минимизация наносимого ущерба, разглашения, изменения, утраты и незаконного тиражирования информации.

Средства обеспечения информационной безопасности представляют собой совокупность правовых, организационных и технических средств, соответственно, предназначенных для обеспечения информационной безопасности. Все средства обеспечения информационной безопасности делятся на две группы:

1. формальные средства, которые выполняют функции по защите информации формально, практически без участия человека, по большей части;
2. неформальные средства, основанные на деятельности человека.

Формальные средства разделяются на физические, аппаратные и программные. Физические включают механические, электронные, электронно-механические устройства и системы, работающие автономно, при этом они создают различные препятствия для дестабилизирующих факторов.

Аппаратные средства – это средства, схематически включаемые в аппаратуру системы обработки данных специально для обеспечения задач по защите информации.

Также проводится ряд мероприятий, целью которых является защита информации, например такие как:

1. распределение реквизитов, разграничивающих доступ к информации (ключей шифрования, паролей и др.);
2. мероприятия по реконструкции построения системы защиты;
3. кадровые изменения в составе персонала системы по подбору и распределению кадров (контроль принимаемых на работу сотрудников, инструктаж по работе с информацией, обучение, ознакомление с мерами ответственности за нарушение правил по защите информации, создание условий, при которых персоналу было бы не выгодно нарушать свои обязанности и др.);
4. противопожарная охрана, охрана помещений организации, создание пропускного режима, организация мер по обеспечению сохранности и физической целостности техники и носителей информации и др.;
5. открытая и тайная проверка работы персонала;
6. контроль над использованием защитных мер;
7. мероприятия по установлению правил разграничивающих доступ пользователей к информации внутри организации.

«В настоящее время критически важным государственным ресурсом, обеспечивающим национальную безопасность, становится информация, циркулирующая в телекоммуникационных и компьютерных системах различного назначения»[1]

Также целый ряд других мероприятий, которые направленны на защиту секретной информации. Кроме организационных мер, важную роль играют

[1] Шубинский М.И. Информационная безопасность для работников бюджетной сферы: Учебное пособие. СПб: СПбГУ ИТМО, 2012. С. 47.

различные меры технического характера (аппаратные, программные и комплексные).

«Документ - материальный носитель с зафиксированной на нем в любой форме информацией в виде текста, звукозаписи, изображения и (или) их сочетания, который имеет реквизиты, позволяющие его идентифицировать, и предназначен для передачи во времени и в пространстве в целях общественного использования и хранения»[1]

В ходе данного исследования становится понятно, что органы внутренних дел уделяют особое внимание сохранности секретных сведений и выработке у сотрудников большей бдительности. Однако, некоторые сотрудники недооценивают тяжесть последствий от утечки тайных сведений. Такие сотрудники проявляют недобросовестное отношение и халатность при работе с тайными документами, из-за чего тайные сведения могут быть разглашены, а также утеряны секретные предметы и документы. При этом некоторые сотрудники поддерживают сомнительные связи, и неформально разглашают важные сведения о способах и методах работы органов внутренних дел. Низкие профессиональные качества таких сотрудников, как правило, приводят к нарушению конспирации проводимых мероприятий.

2.2 Деятельность органов внутренних дел по расследованию преступлений в сфере информационных технологий

«Для возбуждения уголовных дел о преступлениях в сфере компьютерной информации, типичными поводами и основаниями являются:

1. сообщения от потерпевших юридических лиц (предприятий, учреждений и организаций), поступающие от должностных лиц и базирующиеся на материалах контрольно-ревизионных проверок и сообщений служб собственной безопасности;

[1]Федеральный закон «Об обязательном экземпляре документов» от 29 декабря 1994 г. № 77-ФЗ// Российская газета от 17 января 1995 г.

2. заявления от потерпевших физических лиц, самостоятельно обнаруживших факт совершения в отношении их противоправного деяния;

3. непосредственное обнаружение признаков преступления органом дознания в результате:

3.1. проверки сообщения о совершённом или готовящемся преступлении;

3.2. в ходе проведения специальных оперативно-технических мероприятий;

3.3. по материалам инициированных контрольно-ревизионных и иных документальных проверок;

3.4. путём проведения контрольных закупок;

3.5. при непосредственном задержании лица с поличным на месте совершения преступления;

4. статьи, заметки и письма, опубликованные в средствах массовой информации, в том числе электронные, функционирующие в сети Интернет;

5. непосредственное обнаружение признаков преступления дознавателем или следователем при расследовании преступлений другого рода»[1].

Для подготовки и осуществления расследования преступлений в сфере информационных технологий, а также преступлений, использующих сеть «Интернет» крайне эффективно использование результатов оперативно-розыскной деятельности. «Информация, добываемая и используемая в ходе расследования преступлений, представляет собой сведения о лицах, предметах, документах, фактах, событиях, явлениях и процессах, получаемых в порядке, предусмотренном законом «Об оперативно-

[1] Расследование преступлений в сфере компьютерной информации и электронных средств платежа: учебное пособие для вузов / ответственные редакторы В. Б. Вехов, С. В. Зуев. – М.: Издательство Юрайт, 2021. С. 31.

розыскной деятельности» и ведомственными нормативными актами по тактике оперативно-розыскной деятельности»[1]. Эти сведения фиксируются на материальных носителях с реквизитами, позволяющими ее идентифицировать, и сосредотачиваются в информационных системах и делах оперативного учета.

Следует отметить, что при расследовании преступлений в сфере информационных технологий и преступлений с использованием сети «Интернет» наиболее результативно использование статистических данных накопленных органами внутренних дел и информационных ресурсов, формируемых на основе информации, получаемой в ходе ОРМ. «Данная информация образует информационный ресурс оперативных подразделений органов, осуществляющих оперативно-розыскную деятельность, отличающийся конфиденциальным характером. Информация, циркулирующая в оперативно-розыскном процессе, призвана обеспечить решение задач ОРД и содействовать разрешению проблем уголовного процесса»[2].

Получение предварительной информации о противоправных деяниях, совершаемых при помощи открытой телекоммуникационной сети «Интернет», можно разделить на две основные группы:

«Получение сообщений, заявлений, обращений граждан о противоправных деяниях, написанных при помощи электронных форм, расположенных на официальных сайтах МВД России, а также при обращении граждан в территориальные органы внутренних дел»[3].

---

[1]Федеральный закон «Об оперативно-розыскной деятельности» от 12 августа 1995 года № 144-ФЗ // [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_7519/ (дата обращения 12.05.2021)

[2]Овчинский С.С. «Оперативно-розыскная информация» М., 2000. С. 74.

[3]Положение об управлении оперативно-розыскной информации службы криминальной милиции МВД России утверждено Приказом МВД России от 19.03.2002 г. №249// [Электронный ресурс]. URL: www.consultant.ru/cons/cgi/online.cgi?req=doc&base=EXP&n=305411#03590094799605392/ (дата обращения 12.05.2020).

Пример: гражданин G обратился в полицию при помощи электронной формы, расположенной на официальном сайте МВД. В своем обращении он указывает, что им была создана онлайн игра и размещена на сервере хостинг-центра. Своей знакомой он предоставила данные для авторизации через консоль администратора, для осуществления графического оформления. Ее друг, который имел корыстные намерения, попросил загрузить файл, который явился троянской программой типа «бэкдор» (Backdoor -- чёрный вход, задняя дверь) на сервер. После этого он скопировал исходные коды онлайн игры и все базы данных пользователей. Следующим шагом злоумышленник оформил доменное имя и разместил копию игры.

Когда автор игры обнаружил данный инцидент, он нашел троянскую программу на своем сервере и модифицировал ее, в результате чего ему удалось получить электронный почтовый ящик злоумышленника, на который отправлялась информация, а также установить IP-адрес, с которого злоумышленник обращался к своему «бекдору».

Получение информации от граждан, оказывающих негласное содействие сотрудникам полиции. «В основном, информация, предоставляемая гражданами, оказывающих негласное содействие сотрудникам полиции, касается совершением мошеннических действий в сети интернет, так как они зарегистрированы на тематических сайтах и форумах»[1].

Третью группу формирует личный сыск сотрудника подразделения, в чью компетенцию входит рассмотрение компьютерных преступлений. Наиболее широко личный сыск применятся при обнаружении фактов распространения в сети «Интернет» детской порнографии.

«Ключевая особенность компьютерных преступлений заключается в том, что их реализации осуществляется при помощи технических средств,

[1]Белоглазов Е.Г. Основы информационной безопасности органов внутренних дел: Учебное пособие. М.: УМВД России, 2012. С. 47.

таких как персональный компьютер, мобильные или портативные устройства»[1].

«Возможность доступа пользователям предоставляют Интернет-провайдеры. Каждому устройству выделяется IP-адрес, по которому происходит соединение с всемирной сетью «Интернет». При этом происходит регистрация в Log-файле, кому и когда предоставлялся определенный IP-адрес. Поэтому сбор предварительной информации направлен в первую очередь на установления IP-адреса злоумышленника»[2].

Учитывая изложенное, следует представитьпоследовательность расследования преступлений, совершаемых при помощи ОТКС «Интернет».

Установление IP-адреса. Данная информация устанавливается при помощи осуществления официального запроса в организации, предоставляющие различные услуги в сети Интернет: почтовые сервисы (mail.ru, yandex.ru, rambler.ru), социальные сети («ВКонтакте», «Одноклассники»), платежные системы («Яндекс.деньги», «QIWI»), регистраторы доменов (REG.RU, RU-CENTER). Помимо самого IP-адреса, необходимо установить точное время его использования.

Однако стоит отметить тот факт, что опытные пользователи скрывают свои истинные IP-адреса при помощи использования proxy-серверов, что затрудняет дальнейшее получение информации о противоправном деянии. Поэтому используют другие методы для выявления лица, совершившего уголовно-наказуемое деяние

Далее провайдер. Установив, с какого IP-адреса осуществлялся доступ к Интернет-ресурсу, определяем при помощи бесплатного и общедоступного сервиса «Whois?» (whois-service.ru, 2ip.ru/whois/) какому провайдеру принадлежит IP-адрес.Помимо названия провайдера, данный сервис предоставляет его контактную информацию.

---

[1]Громов Г.Р. Очерки информационной технологии / М.: ИнфоАрт, 1993. - С. 22.
[2]Черняков М.В., Петрушин А.С. Основы информационных технологий. Учебник для вузов: М., 2007. С. 26.

Местонахождение компьютера. Провайдер заключает с физическим лицом договор о предоставлении услуг связи. Поэтому у него есть регистрационная база всех его пользователей. Помимо этого, у каждого провайдера ведутся Log-фалы, в которые записывается, какому пользователю, в какой момент времени, выделялся IP-адрес.

«Компьютер. Для установления всей информации, которая может иметь отношении к совершенному компьютерному преступлению, средства вычислительной техники направляют на компьютерно-техническую экспертизу либо исследование. В зависимости от совершенного компьютерного преступления, перед экспертом необходимо поставить конкретные вопросы, ответы на которые будут иметь доказательное значение о причастности владельца компьютера к совершению им незаконных действий при помощи ОТКС «Интернет»»[1].

Личность. Заключающим моментом является установление личности, в чьем пользовании находился компьютер в момент совершения компьютерного преступления.

Применение типологического метода расследования преступлений, совершаемых в сети «Интернет» в практическом подразделении МВД России.Данный метод сбора первичной информации была применена на практике при рассмотрении материала проверки по обращению гр. N.

Фабула противоправного деяния: неустановленное лицо, используя аккаунт в социальной сети, под видом несовершеннолетнего, познакомилось с дочерью гр. N. В ходе общения с несовершеннолетней гр. K, неустановленное лицо попросило выслать ему фотографии интимного содержания. После чего, гр. K, выполнила его просьбу. Заполучив данный фотоматериал, неустановленное лицо разместило их на странице своего аккаунта, тем самым предоставив свободный доступ к их просмотру и

[1]Лопатин В.Н. Информационная безопасность России: Человек. Общество. Государство/ СПб., 2000. С. 23.

возможность их загрузки. Его действиями была нарушена диспозиция п. г, ч. 2, ст. 242.1 УК РФ.

Диспозиция данной статьи затрагивает половую неприкосновенность несовершеннолетних, поэтому необходимо провести ОРМ «Сбор образцов для сравнительного исследования», т.е. загрузить размещенные фотографии на оптический носитель в присутствии двух представителей общественности, провести документирование факта загрузки, опечатать оптический носитель способом, исключающим доступ к нему, и направить для проведения исследования. При этом необходимо поставить перед экспертом ряд вопросов, на которые он должен ответить: имеются ли на представленных фотографиях материалы порнографического содержания? Изображены ли на представленных фотографиях лица несовершеннолетнего возраста?

Сбор предварительной информации в данном случае был начат с направления официального запроса в социальную сеть. В ответ на него Администрация данного Интернет-ресурса предоставила информацию, что указанный пользователь зарегистрировался под никнеймом «Иванов Иван», 01.01.**** года в 00:00:00 по московскому времени, используя IP-адрес 192.168.*.* Также был представлен список времени, даты и IP-адресов, с которых осуществлялось администрирование данного аккаунта.

При помощи сервиса «Whois»был установлен провайдер, которому принадлежит полученный IP-адрес. В ответ на запрос, администрация организации, предоставляющей услуги связи, сообщила, что указанный в запросе IP-адрес01.01.**** года в 00:00:00 по московскому временибыл выделен для доступа в ОТКС «Интернет» абоненту, проживающего по адресу: город S, ул. Свободы, д. 1, кв. 2. Данный абонент был зарегистрирован при оформлении договора как гр.S.

Проведя установочные мероприятия, а именно наведение справок через ЦАСБ (Центральное адресно-справочное бюро) о лицах, зарегистрированных по данному адресу.

В ходе проведения ОРМ «Обследование помещений, зданий, сооружений, участков местности и транспортных средств» был обнаружен и изъят компьютер, с которого осуществлялся доступ в интернет и он был направлен на компьютерно-техническую экспертизу. Данный компьютер принадлежал гр.Q, сожителю гр. S. Вся информация, а также заключения экспертов служит доказательной базой для привлечения гр. Q к уголовной ответственности.

Учитывая вышеизложенное, можно сделать вывод, что предложенная схема по сбору предварительной информации о компьютерном преступлении является эффективной и служит основой для рассмотрения типологического состава преступления.

Рассматривая преступления, касающиеся диспозиции статьи 159 УК РФ, стоит отметить изобретательность злоумышленников в рамках применения нестандартных способов для совершения ими противоправного деяния. Для получения информации по данным фактам требуется больше времени и специальных познаний в различных областях. Одним из главных методов, которым пользуются злоумышленники, является социальная инженерия. При общении с «жертвой» они стараются расположить ее к себе и получить ее доверие.

Наиболее часто социальная инженерия применятся при осуществлении продажи товаров или услуг в сети Интернет. В настоящее время активно развивается следующий способ совершения мошеннических действий: в преступной группе создаются несколько подгрупп, которые выполняют разные функции и они знают о существовании других подгрупп, но лично контакт между собой не осуществляют. Содействие осуществляется через третьих лиц. Функции подразделяются на следующие:

1. организаторы. Осуществляют взаимодействие подгрупп между собой, прибегая к помощи третьих лиц;
2. «отдел кадров». Осуществляет поиск в сети Интернет лиц, обладающих специальными познаниями в сфере компьютерной

информации, а также определенными навыками, требующихся для определенных подгрупп;

3. подгруппа «хакеры». В их обязанности входит поиск и «взлом» аккаунтов распространенных социальных сетей, а также учетных записей «Skype»,«ICQ» и т.п.;

4. подгруппа «социальной инженерии». Используя предоставленные данные, они осуществляют несанкционированную авторизацию через аккаунт пользователя и исследуют диалоги, которые ведутся с другими пользователями. Целью изучения является получение информации о том, кому доверяет «взломанный» пользователь. После этого от его лица ведется диалог с просьбой перевести некоторую сумму денежных средств на номер банковской карты, либо на иной счет платежной системы виртуальной валюты;

5. подгруппа «инкассаторов». Данные лица осуществляют обналичивание денежных средств, либо перевод их на иные счета платежных систем.

Однако наибольшее число мошеннических действий при помощи сети Интернет совершают лица одиночки. В качестве примера по данному виду противоправного деяния приведем обращение гр. N.

На сайте бесплатных объявлений гр. Nнашла объявление о продаже цифрового фотоаппарата стоимостью 15000 рублей. В контактной информации объявления был указан абонентский номер, по которому гр. Nсвязалась с лицом(гр. S), разместившем его. В ходе общения продавец сказал, что отправит товар при помощи службы доставки, после оплаты товара на номер QIWI-кошелька. Продавец получил доверие гр. N, и она совершила платеж через терминал оплаты. После повторного телефонного звонка, гр. S подтвердил, что транзакция прошла успешно и прервал разговор. После этого он перестал отвечать на телефонные звонки и оплаченный товар гр. N доставлен не был.

Используя предложенную последовательность расследования преступлений, были осуществлены официальные запросы в администрацию сайта «Avito.ru»и платежной системы «QIWI»сцелью получения IP-адресов администрирования.

В ответном письме они предоставили данные об IP-адресе, с которого, в одном случае, было размещено электронное объявление, с указанием точного времени, и в другом - IP-адрес администрирования электронного кошелька. Предоставленная информация показала, что IP-адреса идентичны.

Помимо этого, «QIWI» предоставил выписку по счету электронного кошелка, в котором отображалась транзакция поступления денежных средств в размере 15000 рублей с терминала оплаты, котором воспользовалась гр. N.

При помощи сервиса «Whois»было установлено, что данный IP-адрес входит в диапазон IP-адресов, обслуживание которых осуществляет провайдер «Example»в городе М. Данный провайдер предоставил анкетные данные того, кому выделялся указанный IP-адрес. И подтвердил, что в указанный момент времени, он обращался к Интернет-ресурсу «Avito.ru».

Однако IP-адрес не всегда можно идентифицировать. Более опытные пользователи, решившие использовать свои познания в сфере высоких технологий, прибегают к помощи proxy-серверов, что затрудняет сотрудникам специализированных подразделений, осуществлять свою деятельность.

Не смотря на попытки злоумышленников скрыть свою личность, всё же остаются следы их присутствия в сети, методы работы правоохранительных органов позволяют успешно осуществлять розыск преступников даже при минимуме сведений, поэтому необходимо осуществлять сбор всей доступной информации, которую можно получить в рамках проверки.

2.3 Информационные технологии, применяемые в деятельности органов внутренних дел по расследованию преступлений в сфере информационных технологий и средства их обеспечения

На данный момент органы внутренних дел России обладают внушительным массивом оперативно-розыскной и справочной информации, которая необходима сотрудникам правоохранительных органов для проведения следственных и оперативно-розыскных мероприятий, а также для ряда других служебных задач.

«Контроль за соблюдением требований к защите информации и эксплуатацией специальных программно-технических средств защиты, а также обеспечение организационных мер защиты информационных ресурсов, обрабатывающих информацию с ограниченным доступом в негосударственных структурах, осуществляется органами государственной власти»[1]

«В настоящее время современные информационные технологии обеспечивают оперативно-аналитический поиск информации для правоохранительных органов»[2].

«Предполагается, что все составляющие национальных интересов в информационной сфере могут, в свою очередь, рассматриваться как совокупность сбалансированных интересов личности, общества и государства. При этом интересы личности заключаются в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность. Интересы общества заключаются в обеспечении интересов

[1]Вострецова Е.В. Основы информационной безопасности : учебное пособие для студентов вузов / Екатеринбург : Изд-во Урал. ун-та, 2019. С. 56.

[2]Кубов Р.Х. Информационно-аналитическое и методическое обеспечение уголовной политики в сфере противодействия организованным формам преступной деятельности / Российский следователь. 2008. №17 С. 46.

личности в информационной сфере, упрочении демократии, создании правового социального государства, достижении и поддержании общественного согласия, в духовном обновлении России. Интересы государства заключаются в создании условий для гармоничного развития российской информационной инфраструктуры, для реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и социальной стабильности, в безусловном обеспечении законности и правопорядка, развитии равноправного и взаимовыгодного международного сотрудничества»[1]

Без интеграции в деятельность правоохранительных органов новых информационных технологий невозможна их эффективная деятельность по раскрытию и расследованию преступлений в сфере информационных технологий.

Информационно-аналитическое обеспечение деятельности правоохранительных органов представляет собой систему, в которую включены два основных взаимосвязанных элемента, требующие непрерывного внимания.

Первым элементом является информационное обеспечение, заключающееся в изучении информационного спроса потребителей, поддержании информационных сетей в устойчивом состоянии, а также сборе, накоплении, обработке, хранении и выдаче информации пользователям в кратчайшие сроки.

Второй элемент представляет собой аналитическое обеспечение, которое заключается в исследовании криминальных угроз, выявление причин и условий, влияющих на формирование криминальной обстановки,

[1]Городов О. А. Информационное право : учебник для бакалавров / М.: Проспект, 2016. С. 54.

прогнозировании её развития и изучении проблемных ситуаций и препятствий в сфере противодействия организованной преступности.

Классификация информационных технологий и средств их обеспечения:

1. автоматизированные информационные системы и их сети:
   - 1.1. базы данных;
   - 1.2. экспертные системы;
   - 1.3. автоматизированные системы управления;
   - 1.4. системы автоматизированного проектирования;
   - 1.5. информационно-вычислительные системы;
   - 1.6. информационные сети;
2. технические средства:
   - 2.1. средства вычислительной техники;
   - 2.2. средства связи;
   - 2.3. средства телекоммуникации;
   - 2.4. другие технические средства;
3. программные средства:
   - 3.1. операционные системы;
   - 3.2. прикладные программы;
4. лингвистические средства:
   - 4.1. словари;
   - 4.2. тезаурусы;
   - 4.3. классификаторы;
5. организационно-правовые средства:
   - 5.1. положения;
   - 5.2. должностные инструкции;
   - 5.3. нормативно-технические документы;
6. технологическое обеспечение:
   - 6.1. информационные технологии;
   - 6.2. инструкции, правила.

«Работа с электронными носителями информации при проведении следственных действий и оперативно-розыскных мероприятий требует строгой регламентации в законе. Анализ уголовных дел свидетельствует о том, что на законодательном уровне решены далеко не все проблемные вопросы»[1].

«Необходимо учитывать, необходимость неотложного решения задач по стабилизации преступлений в сфере информационных технологий. Исходя из этого, оперативно-розыскная деятельность в сфере информационных технологий должна соответствовать развитию электронно-вычислительной техники. Стратегия и тактика оперативно-розыскной деятельности в области информационных технологий должна базироваться на основе максимально широкого использования современных достижений в данной области»[2].

На этапе разработки стратегии и тактики оперативно-розыскной деятельности в области информационных технологий необходимо гласно и негласно привлекать высококвалифицированных специалистов сведущих в данной сфере. Также, при осуществлении агентурной работы, необходимо существенно пересмотреть качественный состав при установлении конфиденциального сотрудничества.

Одним из ключевых моментов является потребность в пополнении арсенала оперативной техники современными техническими приборами, устройствами и компьютерными программами, разработанными и успешно применяемыми в информационно-технологической сфере народного использования. Личному составу специализированных оперативных подразделений необходимо пройти соответствующую подготовку по использованию данной техники.

---

[1]Основы теории электронных доказательств: монография / под ред. докт. юрид. наук С.В. Зуева. М., 2019. С. 9.

[2]Степанов О. А. Правовые основы обеспечения охранительной функции государства в условиях использования новых информационных технологий: Учебное пособие. М.: Академия управления МВД России, 2012. С. 84.

Если не использовать самые современные технические средства, эффективность оперативно-розыскной деятельности в сфере информационных технологий непременно снизится. Подразделения органов внутренних дел могут использовать как универсальное, так и специальное программное обеспечение.

Универсальные программы общего назначения (электронные таблицы, информационно-поисковые системы, редакторы и др.) повышают производительность труда и эффективность работы по выявлению, раскрытию и расследованию преступлений, а также поднимают её на качественно новый уровень.

Специализированные программы ориентированы и применяются непосредственно при осуществлении оперативно-розыскных мероприятий в направлении борьбы с информационной преступностью.

На данный момент уже существует множество программ, с огромным спектром возможностей, позволяющих:

1. контролировать процесс попыток взлома компьютерной системы или сети;
2. определять идентификационные характеристики программ и индивидуальный почерк работы программиста;
3. определять перечень электронных адресов и сайтов, с которыми работал пользователь;
4. негласно регистрировать перечень программ, используемых пользователем;
5. определять путь, при возможности, конкретный адрес с которого исходит угроза компьютерным системам;
6. осуществлять негласное наблюдение за действиями программиста, определив характер разрабатываемых продуктов;
7. обнаруживать скрытую и закодированную информацию в компьютерной системе;

8. осуществлять исследование следов деятельности автора с целью идентифицировать его;

9. осуществлять диагностику устройств и систем на возможность несанкционированного доступа к ним.

Это далеко не полный перечень возможностей существующего программного обеспечения, которое может успешно применяться в ходе расследования преступлений в сфере информационных технологий.Помимо информационных систем, создаваемых и применяемых органами, осуществляющими оперативно-розыскную деятельность, имеет огромный потенциал применение данного программного обеспечения с целью добывания информации.

Поисковые программные средства могут широко применяться в оперативно-розыскной деятельности в непроцессуальной форме, в том числе и до возбуждения уголовного дела. Основанием возбуждения уголовного дела и производством расследования может послужить факт обнаружения программного обеспечения для изготовления вирусов или для осуществления взлома компьютерных сетей. В процессуальной форме поисковые программные средства могут применяться при проведении следственных действий, как пример осмотр места происшествия, личный осмотр, выемка предметов, документов и электронной почтовой корреспонденции, а также при проведении следственного эксперимента, выполняемые с целью опытной проверки показаний.

Одной из своих целей государство ставит «совершенствование системы информационно-аналитического обеспечения принимаемых решений на всех уровнях государственного управления, обеспечение оперативности и полноты контроля за результативностью деятельности органов

государственной власти и обеспечение требуемого уровня информационной безопасности электронного правительства при его функционировании»[1]

Изучение принципов применения информационных технологий в ОВД подразумевает изучение законов развития правоохранительных систем, а также закономерностей информации социального управления.

Под законом понимается порядок необходимой и прочной связи между явлениями и свойствами социальных объектов, их существенные повторяющиеся отношения. Под закономерностью понимается повторяющиеся устойчивые связи и отношения между явлениями, которые определяют объективные условия существования и развития определённого социального процесса. Закономерность является формой конкретного проявления объективно существующего закона.

Изучение законов и законов и закономерностей управления ОВД осуществляется за счёт академических курсов по теории управления ОВД, организации управленческой деятельности в органах внутренних дел и соответствующей учебной и методической литературы.

Касательно законов и закономерностей информационно-технологического обеспечения управления ОВД необходимо учесть недостаточную степень их изученности и исследования. Закономерности построения и функционирования информационных технологий управления, направленных на достижение их социальных целей, на данный момент находится на стадии теоретического осмысления, что сопровождается научно-практическими исследованиями.

Организация информационных технологий управления в сфере правоохранительной деятельности обусловлена особенностями информационного обеспечения. Эта закономерность вытекает из необходимости разнообразия. Объектом информационного обеспечения

[1]Концепция формирования в Российской Федерации Электронного правительства до 2010 года от 6 мая 2008 г.// [Электронный ресурс]. URL:https:// www.consultant.ru/document/cons_doc_LAW_76942/(дата обращения 12.05.2021).

выступает система управления ОВД. При детальном рассмотрении круга объектов информационного обеспечения становится понятно, что их перечень превышает соответствующий перечень объектов управления.

Данный факт обусловлен тем, что содержание информационного обеспечения относится ко всему процессу управления, к отдельным его стадиям и функциям, методам и формам, к деятельности определённых управленческих звеньев, к конкретным видам управляемой правоохранительной деятельности и к деятельности конкретных категорий сотрудников ОВД и военнослужащих внутренних войск. В каждом из приведённых случаев информационные технологии обеспечения будут характеризоваться своей спецификой и особенностями. Как пример, информационно-технологическое обеспечение управленческих функций системы органов внутренних дел дифференцируется на информационные технологии прогнозирования, планирования, организации и контроля.

Также закономерна непрерывность и цикличность информационно-технологического обеспечения процесса управления в сфере правоохранительной деятельности. Информационные технологии управления органами внутренних дел обеспечивают ряд повторяющихся взаимосвязанных операций по сбору, хранению, обработке, передаче и предоставлению информации, что обеспечивает неразрывность управленческих процедур во времени, цикличный переход от одной управленческой функции к другой.

Также является закономерностью функциональная специализация информационных технологий управления органами внутренних дел, которая происходит по мере усложнения сферы правоохранительной деятельности. Эта закономерность прямо связана с динамикой социального развития и особенностями прогресса компьютерной индустрии. Традиционные общепринятые схемы информационного обеспечения правоохранительной деятельности в условиях прогрессирующего общества всё чаще оказываются неэффективными и преобразуются в специализированные комплексы и

подсистемы. Благодаря пониманию данной закономерности можно успешно решать вопросы соотношения централизации и децентрализации информационно-технологического обеспечения ОВД, создания и функционирования информационных технологий, направленных на функциональную специфику решения неоднородных управленческих задач в различных регионах России.

Следует заострить внимание на технологическом консерватизме информационного обеспечения правоохранительной деятельности по сравнению с динамичными и изменчивыми процессами управления. Из практики деятельности ОВД последнего десятилетия, существующие структуры информационно-технологического обеспечения неизбежно устаревают, при этом отмечается нарастание скорости старения. Из этого можно сделать очевидный вывод, что технологические преобразования должны быть адаптивны меняющимся целям и соответствующим им функциям управления.

Объективные закономерности информационного обеспечения управления ОВД не исчерпываются приведенным кратким перечнем. Познание технических закономерностей - это процесс познания объективной реальности развития общества с присущими ему противоречиями и сложностями.

Переходя к рассмотрению принципов построения и применения информационных технологий в деятельности ОВД, отметим, что они служат основой практической реализации объективных законов и закономерностей в процессе жизнедеятельности правоохранительных систем. Именно поэтому рассмотрению информационно-технических принципов управления всегда должен предшествовать анализ соответствующих законов и закономерностей.

Под принципами информационно-технологического обеспечения управления ОВД следует понимать императивы, правила, постулаты и общие идеи о том, как должна строиться, функционировать и развиваться система

информационных технологий в сфере правоохранительной деятельности. В отличие от закономерностей, принципы субъективны по своей природе. Они формируются специалистами на основе познания закономерностей и опыта практической деятельности. С точки зрения гуманитарных, социальных наук именно люди создают, формируют принципы, идеи и категории соответственно своим общественным отношениям и своей коммуникативной практике.

К настоящему времени исследован и обоснован достаточно широкий круг принципов создания и применения информационных технологий в деятельности ОВД. Целесообразно разделить его на три взаимосвязанные принципиальные группы:

1. основополагающие организационно-технологические принципы информационного обеспечения деятельности ОВД;
2. методологические принципы создания автоматизированных информационных систем ОВД всех видов и уровней на основе современных компьютерных технологий;
3. принципы информатизации управления ОВД и ВВ.

Рассмотрим указанные выше принципы более подробно. Содержание первой группы принципов следует из обоснованных признаков, которыми должна характеризоваться всякая научная и практическая технология, а также из обоснованных критериев, которым эта технология должна отвечать.

Принцип разделения процесса информационного обеспечения в деятельности ОВД на внутренние взаимосвязанные этапы является одним из основополагающих с позиций научной технологии. В этом принципе заложено объективное стремление социальной системы обеспечить оптимальную или близкую к оптимальной динамику развития процесса информационного обеспечения. Практическое использование данного принципа позволяет определить рациональные границы требований к личному составу, который будет действовать по данной информационной технологии на каждом этапе управленческого процесса.

Принцип координированного и поэтапного выполнения целенаправленных действий по информационному обеспечению деятельности ОВД базируется на внутренней логике процесса управления. Соблюдение данного принципа позволяет достичь цели информационной технологии - получение информации, полностью удовлетворяющей требованиям системы управления.

Принцип однозначности выполнения включенных в информационную технологию процедур и операций отражает непременное и решающее условие достижения результатов, адекватных поставленной цели. Соблюдение этого принципа требует разработки и неукоснительного выполнения внутрисистемных норм и нормативов обработки информации в структуре МВД России. Только в этом случае вся совокупность управленческих, оперативно-справочных, розыскных, криминалистических и иных служебных данных будет характеризоваться единообразием и пригодностью к использованию в любой географической точке системы на любом уровне управления. Разработка, внедрение и практическое использование единой системы норм и нормативов являются научной основой, необходимым условием для проектирования любых информационных технологий в органах внутренних дел и внутренних войсках.

Принцип массовости информационного продукта в деятельности ОВД определяет перерастание информационного обеспечения из второстепенной обеспечивающей функции в мощный компонент управления. Основное значение массовости продукта информационной технологии для развития системы управления правоохранительной деятельности состоит в том, что такая система требует строгой воспроизводимости результатов.

Именно строгая воспроизводимость «серийного» производства информации (но не стереотипность самой информации) отличают научно обоснованную технологию информационного обеспечения деятельности

ОВД от искусства отдельных аналитиков-детективов, прославившихся со времен дореволюционной российской полиции.

Принцип предельности параметров информационного продукта в системе управления ОВД и ВВ характеризует соотношение между реально достигнутыми и предельно возможными характеристиками информации.

Аналогично этот принцип относится и к информационно-технологическому процессу обеспечения правоохранительной деятельности. В достаточно сложных информационных массивах МВД России существуют как очевидные физические ограничения (объем накопителя, плотность записи, скорость обработки и передачи данных), так и менее очевидные системные ограничения.

Системные ограничения (системная сложность информационного продукта, базы данных) определяются уже информационно-технологическими принципами управления. Причем такие ограничения имеют как абсолютный характер, так и физические законы.

Принцип сложности информационного продукта в системе управления ОВД тесно связан с предыдущим принципом предельности параметров. Суть его состоит в том, что невозможно воспроизводить ни один информационный результат высокого уровня сложности и качества, не повторив всю технологию его получения.

Например, для того, чтобы воспроизвести, повторить оценку оперативной обстановки на территории государства по итогам календарного года, необходимо еще раз собрать всю совокупность данных о преступности и правонарушении, о причинах, условиях и факторах, определяющих криминологические процессы, о силах и средствах ОВД, о показателях эффективности правоохранительной деятельности. Вновь собранные данные следует агрегировать, интегрировать и подвергнуть обработке в соответствии с установленными критериями и затем представить по установленной форме.

Таким образом, перечисленные шесть организационно-технологических принципов информационного обеспечения деятельности

ОВД постулируют замену традиционной концепции выбора методов, приемов, средств работы с информацией.

«Права доступа определяют набор действий (например, чтение, запись, выполнение), разрешённых для выполнения субъектам (например, пользователям системы) над объектами данных. Для этого требуется некая система для предоставления субъектам различных прав доступа к объектам. Это система разграничения доступа субъектов к объектам, которая рассматривается в качестве главного средства защиты от несанкционированного доступа к информации»[1].

Вместо произвольной (зачастую искусной, а иногда и очень качественной) комбинаторики приемов обработки данных, подготовки и пересылки бумажных документов, формирования многоярусных картотек и многоэтажных архивов формируется научная стратегия выбора оптимальной структуры информационного продукта и рациональной последовательности этапов его синтеза и использования. При этом важно учитывать, что существует строго однозначное соответствие между системными принципами информационной технологии, качеством исходных данных и функциональными характеристиками конечного информационного продукта.

На сегодняшний день, установились главные задачи отдела по борьбе с преступлениями в сфере информационных технологий. Своевременное обнаружение преступлений в области компьютерной информации, если в качестве объекта преступного посягательства выступает ЭВМ, а также сети и системы права владельца информации, а также посягательств на конституционное право граждан - тайну переписки, неприкосновенность приватной жизни, тайну телефонных переговоров, телеграфных и почтовых уведомлений, осуществленных посредством прослушивания или прочтения сообщений.

[1]Аверченков В.И., Рытов М.Ю. Организационная защита информации: учебное пособие / М.: Флинта, 2011. С. 37.

Возбуждение уголовного дела или производства неотложных следственных мероприятий, а также, в случае необходимости, активное пресечение таких нарушений.

Обнаружение сообществ, групп или отдельных лиц, которые занимаются противоправной деятельностью в указанной сфере, надлежащее документирование проводимой ими преступной деятельности, разработка и реализация мероприятий, направленных на предупреждение преступлений такого рода.

Выполнение различных поручений следователей по анализу и расследованию таких преступлений, проведение оперативно-розыскной деятельности и участие следственно-оперативной группы в расследовании таких преступлений.

Подразделения подобного рода созданы и функционируют также и в других правоохранительных органах Российской Федерации, на пример, в ФСБ и Генеральной прокуратуре. Имея при этом ряд специализированных задач.

Аналитическая разведка совершенствования аналитического и информационного обеспечения деятельности соответствующих подразделении криминальной полиции, исследование перспективных методов и средств поиска и проведение сопоставительного анализа информации, которая имеет значение в борьбе с указанным видом преступлений. Главная цель такого анализа заключается в формировании новых знаний о методах и способах осуществления неправомерного доступа к информационным сетям и компьютерной информации и способы его сокрытия.

«Обеспечение высокого уровня информационной безопасности внутренних правоохранительных органов, который включает в себя защиту субъектов, прав и интересов правоохранительных органов от некачественной либо устаревшей информации и защиту ведомственной информации, имеющей ограниченный доступ, информационных технологий и прочих

технических средств их обеспечения. Так, информационная безопасность ОВД характеризуется надежностью систем ее обеспечения, в том числе надежностью программного обеспечения и аппаратных средств»[1].

В ходе написания второй главы были рассмотрены вопросы, связанные с противодействием органов внутренних дел преступлениям в сфере информационных технологий. Кратко были раскрыты типичные методы совершения киберпреступлений, далее была отражена деятельность органов внутренних дел при расследовании таких преступлений, выделены этапы данной деятельности, раскрыты методы и приведены практические примеры.

Информация, накапливаемая и хранящаяся в информационных системах ОВД, является конфиденциальной. Учитывая скорость развития технологий, возникает проблема вероятной угрозы информации важной для деятельности правоохранительных органов. Исходя из этого, уровень информационной безопасности в ОВД должен обладать высокой надёжностью и сочетать в себе технические, программные и организационные средства обеспечения.

Также был раскрыт вопрос об информационных технологиях, применяемых в деятельности органов внутренних дел. Была дана классификация применяемых технологий и средств их обеспечения. Следует выделить проблему необходимости интеграции в деятельность ОВД самых современных технологических достижений. Данная проблема решается достаточным финансированием, также проводятся курсы обучения и переобучения для сотрудников, разрабатываются необходимые инструкции и правила по использованию информационных технологий.

[1]Жуков Ю.И., Приманкин А.И., Щербаков О.В. Информационная безопасность и аппаратно-программная надежность компьютерных средств органов внутренних дел // Вестник МВД России. 2010. №3. С.77.

ЗАКЛЮЧЕНИЕ

В ходе данного исследования, мы дали определение информации, информационных технологий и преступлений в сфере информационных технологий. Также были раскрыты методы борьбы правоохранительных органов с подобными преступлениями, перечислены препятствия мешающие расследованию и выделены наиболее серьёзные проблемы, как для информационного общества, так и для деятельности правоохранительных органов в сфере информационных технологий. Исследуя данные проблемы, постепенно были найдены направления развития для их устранения.

С формированием современной информационной среды представляется множество возможностей для совершения преступлений, также появляются всё новые формы и способы противостояния деятельности правоохранительных органов в расследовании преступлений. В данном случае проблема касается не только расследования преступлений в сфере информационных технологий. Чем больше общедоступной информации злоумышленник получает о методах расследования преступлений, тем меньше следов он оставит и ошибок допустит при совершении преступления. Сейчас можно смело утверждать о том, что на вооружение преступников взяты функциональные возможности информационных технологий, которые они используют для повышения эффективности сокрытия преступной деятельности и своей личности. Гипотетический пример, убийца планирует вывезти труп за пределы города, он откроет приложение в телефоне, выяснит расположение сотрудников ДПС и сможет избежать их. Однако с развитием и использованием информационных технологий правоохранительные органы также получили возможность повысить эффективность своей деятельности. Впоследствии, выяснить личность преступника станет только проще, отследив его перемещение.

В ходе исследования становится ясно, что деятельность органов внутренних дел по расследованию преступлений в сфере информационных

технологий требует значительного финансирования, активного привлечения специалистов и интеграции современных технологий. Гораздо меньше ресурсов требуется на то, чтобы информация не была подвергнута несанкционированному доступу, что обеспечивается применением разработанных методов обеспечения информационной безопасности. Что естественно, предупреждение преступления требует меньше сил и средств, чем его раскрытие.

Исходя из вышесказанного, вытекает следующая проблема, а именно технологический консерватизм информационного обеспечения правоохранительной деятельности по сравнению с динамичными и изменчивыми информационными процессами. Из этого можно сделать очевидный вывод, что технологические преобразования должны быть адаптивны меняющимся целям и задачам правоохранительных органов.

Без интеграции в деятельность правоохранительных органов новых информационных технологий невозможна их эффективная деятельность по раскрытию и расследованию преступлений в сфере информационных технологий. В сравнении с обычными пользователями компьютеров и мобильных телефонов, технологическое обеспечение правоохранительных органов гораздо выше, что только облегчает ход расследования. Напротив, сведущие в информационных технологиях преступники, а также обладающие примерными представлениями о методах расследования значительно затрудняют ход расследования преступлений.

Для подготовки и проведения расследования преступлений в сфере информационных технологий важную роль играет информация, добываемая в ходе оперативно-розыскной деятельности. Стоит отметить, что наиболее активно используются технические средства, обеспечивающие добывание информации, именно в данной деятельности. Стратегия и тактика оперативно-розыскной деятельности в области информационных технологий должна базироваться на основе максимально широкого использования современных достижений в данной области. Личному составу

специализированных оперативных подразделений необходимо пройти соответствующую подготовку по использованию данной техники. Если не использовать самые современные технические средства, эффективность оперативно-розыскной деятельности в сфере информационных технологий непременно снизится.

Будет неверным заявление, что правоохранительные органы бездействуют в данном направлении и не стремятся решить эту проблему. Информационно-аналитическое обеспечение деятельности правоохранительных органов представляет собой систему, в которую включены два основных взаимосвязанных элемента, требующие непрерывного внимания. Первым элементом является информационное обеспечение, заключающееся в изучении информационного спроса потребителей, поддержании информационных сетей в устойчивом состоянии, а также сборе, накоплении, обработке, хранении и выдаче информации. Второй элемент представляет собой аналитическое обеспечение, которое заключается в исследовании криминальных угроз, выявление причин и условий, влияющих на формирование криминальной обстановки, прогнозировании её развития и изучении проблемных ситуаций и препятствий в сфере противодействия организованной преступности.

Довольно серьёзной проблемой является объединение и организация преступников, создание крупных преступных сообществ обеспечивается относительной анонимностью. Информация о преступной деятельности подобных организаций может быть вполне доступна, и в то же время правоохранительные органы не в состоянии установить личности руководителей данных организаций. Как пример действующее в России сообщество «Hydra» где активно продаются наркотические вещества. Оборот средств на данной интернет-платформе за 2020 год составил 1.4 миллиарда рублей. Однако выяснить личности руководителей данной интернет-платформы и прекратить их преступную деятельность правоохранительные органы не в силах.

Одним из наиболее важных вопросов остаётся обеспечение информационной безопасности самих правоохранительных органов, различных организаций и отдельных лиц. Ошибочно относить это к проблеме, так как в данном направлении информационная безопасность обеспечивается целым рядом технических, организационных и правовых мер. В данном исследовании наиболее интересны правовые меры, включающие в себя разработку, а затем внедрение правовых норм, устанавливающих уголовную ответственность за преступления такого рода, защиту авторских прав программистов, усовершенствование гражданского и уголовного законодательства и судопроизводства.

Хоть и были указаны направления для преодоления выделенных проблем, наиболее существенное действие в положительном направлении окажет повышение адаптивности системы правоохранительных органов к изменяющимся условиям современного мира, что повлечёт за собой повышение эффективности их деятельности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

РАЗДЕЛ 1 НОРМАТИВНЫЕ ПРАВОВЫЕ АКТЫ И ИНЫЕ ОФИЦИАЛЬНЫЕ АКТЫ

1. Конституция Российской Федерации, принята всенародным голосованием 12 декабря 1993 г. с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 г. // Российская газета. 2020. № 144.
2. Окинавская Хартия глобального информационного общества// Дипломатический вестник. 2000. №8. Ст. 52.
3. Гражданский кодекс РФ (Ч. II) от 26 января 1996 г. № 14-ФЗ // [Электронный ресурс].URL: www.consultant.ru/document/cons_doc_LAW_9027/(дата обращения 12.05.2020).
4. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ //[Электронный ресурс].URL: www.consultant.ru/document/cons_doc_LAW_10699/(дата обращения 12.05.2020).
5. Федеральный закон «Об оперативно-розыскной деятельности» от 12 августа 1995 года № 144-ФЗ // [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_7519/(дата обращения 12.05.2020).
6. Федеральный закон Российской Федерации «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года №149-ФЗ// СЗ РФ. 2006. № 31. Ст. 3448.
7. Федеральный закон Российской Федерации «Об электронной цифровой подписи»от 10 января 2002 года №1-ФЗ// Российская газета. 2011. №75.
8. Закон РФ «О государственной тайне» от 21 июля 1993 г. № 5485-I// Российская газета. 2010. № 262.
9. Федеральный закон «О коммерческой тайне» от 29 июля 2004 г. № 98-ФЗ// Российская газета. 2004. № 3543.

10. Федеральный закон «Закон о средствах массовой информации» от 27 декабря 1991 года № 2124-1 ФЗ// Российская газета. 2007. № 213.
11. Федеральный закон «О персональных данных» от 27 июля 2006 г. №152-ФЗ // Российская газета. 2006. № 4131.
12. Федеральный закон «Об обязательном экземпляре документов» от 29 декабря 1994 г. № 77-ФЗ// Российская газета от 17 января 1995 г.
13. Доктрина информационной безопасности Российской Федерации: утверждена Президентом Российской Федерации от 9 сент. 2000 г. №Пр-1895//[Электронный ресурс]. URL:https://base.garant.ru/182535/(дата обращения 12.05.2020).
14. Концепция формирования в Российской Федерации Электронного правительства до 2010 года от 6 мая 2008 г.// [Электронный ресурс]. URL: : https:// www.consultant.ru/document/cons_doc_LAW_76942/(дата обращения 12.05.2020).
15. Концепция использования информационных технологий в деятельности федеральных органов государственной власти до 2010 года// [Электронный ресурс]. URL: https://digital.gov.ru/ru/documents/3017/(дата обращения 12.05.2020).
16. Концепция управления государственными информационными ресурсами: Рекомендована Правительством Российской Федерации для использования при разработке федеральных программ по формированию общедоступных государственных информационных ресурсов// [Электронный ресурс]. URL: http://www.elrussia.ru/166776/(дата обращения 12.05.2020).
17. Электронная Россия (2002-2010 годы): Федеральная целевая программа// [Электронный ресурс]. URL: http://digital.gov.ru/ru/activity/programs/6/(датаобращения 12.05.2020).
18. Вопросы Министерства юстиции Российской Федерации Указ Президента РФ от 13 октября 2004 г. №1313// [Электронный ресурс]. URL:www.consultant.ru/document/cons_doc_LAW_49892/ (дата обращения 12.05.2020).

19. Положение об управлении оперативно-розыскной информации службы криминальной милиции МВД России утверждено Приказом МВД России от 19.03.2002 г. №249// [Электронный ресурс]. URL:www.consultant.ru/cons/cgi/online.cgi?req=doc&base=EXP&n=305411#035 90094799605392/ (дата обращения 12.05.2020).
20. Всемирная встреча на высшем уровне по вопросам информационного общества (World Summit on the Information Society - WSIS) Всемирный Саммит по информационному обществу// [Электронный ресурс]. URL:www.humanities.edu.ru/db/ msg/47695/ (дата обращения 12.05.2020).

РАЗДЕЛ II ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА

1. Абромович, А.М. Диалектика правовой информатизации/ А.М. Абромович - заместитель Главы Администрации Президента Республики Беларусь, д.ю.н., профессор // Современные компьютерные технологии в системах правовой информации: тез. докл. конф., г. Минск, 21-22 нояб. 2002 г. [Электронный ресурс] URL: http://ncpi.gov.by/Conf/tezis.asp? 3/ (дата обращения 17.05.2020).
2. Аверченков, В.И. Организационная защита информации: учебное пособие / В.И. Аверченков, М.Ю. Рытов. М.: Флинта, 2011. 247 с.
3. Антопольский,А.А. Правовое регулирование информационных объектов. Проблемы информатизации. М.: 1999. 347 с.
4. Антонюк, Б.Д. О проблемах законодательного регулирования деятельности в сфере информационных технологий и связи/ Б.Д. Антонюк - заместитель министра информационных технологий и связи Российской Федерации. - М., 2005. [Электронный ресурс] URL: http://www.infolaw.ru/lib/2005-3-legal-regulation-problems/(дата обращения 17.05.2020).
5. Бачило, И.Л. Информационное право: учебник для вузов по направлению подготовки «юриспруденция» специальностям «юриспруденция» и «правоохранительная деятельность» / И.Л. Бачило, В.Н. Лопатин, М.А. Федотов; Министерства науки и образования РФ. - СПб., 2005. - 725 с.

6. Белкин, Р.С. Криминалистика: учебник для вузов / под ред. Р.С. Белкина. – М.: НОРМА, 2001. 990с.
7. Белоглазов, Е.Г., Борзунов К.К., Овчинский А.С. « Применение информационных технологий в аналитической разведке». Московский Университет МВД России, 2005. 237 с.
8. Белоглазов, Е.Г. Основы информационной безопасности органов внутренних дел: Учебное пособие. - М.: УМВД России, 2012. 273 с.
9. Бугроменко, В.Н. TERRA SOCIUM / Бугроменко В.Н. // Социс. 1992. №11. 70. с.
10. Вехов, В.Б., Зуев, С.В. Расследование преступлений в сфере компьютерной информации и электронных средств платежа: учебное пособие для вузов / ответственные редакторы Вехов В.Б., Зуев С. В.. – М.: Издательство Юрайт, 2021. 243 с.
11. Волынский, А.Ф, Криминалистика: Учебник для вузов / под ред. А.Ф. Волынского. - М.: Закон и право, ЮНИТИ-ДАНА, 1999. 615 с.
12. Вострецова, Е.В. Основы информационной безопасности : учебное пособие для студентов вузов / Е.В. Вострецова. Екатеринбург : Изд-во Урал. ун-та, 2019. 204 с.
13. Голубков, А. Концепция формирования и развития единого информационного пространства России и соответствующих информационных ресурсов / А. Голубков // Вестник Российского общества информатики и вычислительной техники: научно-информативный журнал / ВИМИ. 1995. №4. С. 33 – 58.
14. Городов, О.А. Основы информационного права России учеб. пособие / О.А. Городов. - СПб.: Юридический центр Пресс, 2003. С. 17 – 18.
15. Городов, О. А. Информационное право : учебник для бакалавров / Городов О. А. –М.: Проспект, 2016. 304 с.
16. Гринберг, Е.А. «Преступления против общественной безопасности» Свердловск, 1974. 432 с.

17. Громов, Г.Р. Очерки информационной технологии [Текст] / Г.Р. Громов - М.: ИнфоАрт, 1993. 22. с.
18. Доронин, А.И. Разведывательное и контрразведывательное обеспечение финансово-хозяйственной деятельности предприятия / А.И. Доронин. Тула, 2000. 345 с.
19. Емельянов, Г. В. Информационная безопасность России. Основные понятия и определения. Учебное пособие / Под общ. ред. проф. А. А. Прохожева. М.: РАГС при Президенте РФ, 2009. 285 с.
20. Жаров,А.С. Правовые аспекты информационной безопасности: новые подходы / А.С. Жаров // Национальные интересы. - 2005. - №2. 32. с.
21. Жуйков, А.А. Основы информационной безопасности в органах внутренних дел. Словарь терминов и понятий / А.А. Жуйков. Новороссийск : Новороссийский филиал КрУ МВД России, 2014. 113 с.
22. Жуков, Ю.И., Приманкин А.И., Щербаков О.В. Информационная безопасность и аппаратно-программная надежность компьютерных средств органов внутренних дел // Вестник МВД России. 2010. №3. С.42–45.
23. Журавленко, Н.И. Кадулин Б.Е. Основы информационной безопасности: Учебное пособие. - М.: Мос УМВД России. 2012. 254 с.
24. Зегжда, Д.П., Ивашко А.М. Основы безопасности информационных систем. - М.: Горячая линия-Телеком, 2010. С. 20–30.
25. Зуев, С.В. Основы теории электронных доказательств: монография / под ред. докт. юрид. наук С.В. Зуева. М., 2019. С. 9–10.
26. Зуев, С.В. Информация как межотраслевая правовая категория. 1-я видеолекция // [Электронный ресурс]. URL: http://www.iuaj.net/node/2636/(дата обращения 17.05.2020).
27. Каторин, Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина - СПб: НИУ ИТМО, 2012. 416 с.

28. Кемпф, В.А. Основы информационной безопасности органов внутренних дел: учеб. пособие / В. А. Кемпф. Барнаул : Барнаульский юридический институт МВД России, 2014. 104 с.
29. Колин, К.К. Информационная глобализация общества и гуманитарная революция / К.К. Колин // Alma mater (Вестник высшей школы). 2002. №8. 34. с.
30. Копылов, В.А. Информационное право: вопросы теории и практики / В.А. Копылов. - М., 2003. 240 с.
31. Крутских, А.В. Международное сотрудничество в области информационной безопасности / Крутских А.В., Сафронова И.Л. - М., 2003. 229 с.
32. Кубов, Р.Х. Информационно-аналитическое и методическое обеспечение уголовной политики в сфере противодействия организованным формам преступной деятельности / Р.Х. Кубов, кандидат юридических наук / Р.Х. Кубов // Российский следователь. 2008. №17 С. 46
33. Куприянова, Г.И. Информационные ресурсы INTERNET / Г.И. Куприянова. - М.: ИПК госслужбы, 1998. 56 с.
34. Красненкова, Е.В. Обеспечение информационной безопасности в Российской Федерации уголовно-правовыми средствами: дис. канд. юрид. наук: / Е.В. Красненкова. М., 2006. 188 с.
35. Левин, В.К. Концепция развития безопасных информационных технологий: обеспечение защиты информации в проектах информатизации России / Левин В.К. и др.; Министерство науки РФ. М., 1992. 344 с.
36. Лопатин, В.Н. Информационная безопасность России: Человек. Общество. Государство/ В.Н. Лопатин. - СПб., 2000. 23. с.
37. Лопатина, Т.М. Виктимологическая профилактика преступлений в сфере компьютерной информации // Современное право. № 7. 2005. 52. с.
38. Мазуров, В.А. Компьютерные преступления: классификация и способы противодействия. М., 2002. 21. с.

39. Макаров, В.А. Концептуальные основы обеспечения безопасности информации на объектах органов внутренних дел Российской Федерации учеб. пособие / В. А. Макаров. Домодедово : ВИПК МВД России, 2014. 52 с.
40. Министерство внутренних дел РФ характеристика состояния преступности в Российской Федерации[Электронный ресурс] URL:https://мвд.рф/reports/item/22678184/(дата обращения 17.05.2020).
41. Нестеров, С.А. Информационная безопасность и защита информации: Учебное пособие. СПб.: Изд-во Политехн. ун-та, 2009. 126 с.
42. Нестеровский, О.И. Основы информационной безопасности в ОВД: методические рекомендации / О.И. Нестеровский. Электр. дан. и прогр. Воронеж : Воронежский институт МВД России, 2015. 29 с.
43. Овчинский, С.С. «Оперативно-розыскная информация» М., 2000. 164 С.
44. Общество Тасс // [Электронный ресурс]. URL: //tass.ru/obschestvo/903239/ (дата обращения 17.05.2020).
45. Ржавский, К.В. Информационная безопасность: практическая защита информационных технологий и телекоммуникационных систем: Учебное пособие. Волгоград: Изд-во ВолГУ, 2002. 122 с.
46. Советов, Б. Я. Информационные технологии : учебник для среднего профессионального образования / Б. Я. Советов, В. В. Цехановский. 7-е изд., перераб. и доп. М.: Издательство Юрайт, 2019. 327 с.
47. Степанов, О. А. Правовые основы обеспечения охранительной функции государства в условиях использования новых информационных технологий: Учебное пособие. М.: Академия управления МВД России, 2012. 264 с.
48. Федоров, В. Компьютерные преступления: выявление, расследование и профилактика // Законность. № 6. 2004. С. 44.
49. Черняков, М.В., Петрушин А.С. Основы информационных технологий. Учебник для вузов: - М., 2007. 282 с.
50. Шубинский, М.И. Информационная безопасность для работников бюджетной сферы: Учебное пособие. СПб: СПбГУ ИТМО, 2012. 102 с.

РАЗДЕЛ IIIПОСТАНОВЛЕНИЯ ВЫСШИХ СУДЕБНЫХ ИНСТАНЦИЙИ МАТЕРИАЛЫ ЮРИДИЧЕСКОЙ ПРАКТИКИ

1. Постановление Пленума Верховного Суда Российской Федерации «О практике применения судами Закона Российской Федерации «О средствах массовой информации»» от 15 июня 2010 г. № 16// Российская газета. 2010. №132.
2. Постановление Пленума Верховного Суда РФ «Об открытости и гласности судопроизводства и о доступе к информации о деятельности судов» от 13 декабря 2012 г. № 35// Российская газета. 2012. № 292.
3. Приговор суда № 1-609/2017 по обвинению Житникова Д.Апо ч. 2 ст. 272 УК РФ / архив Чкаловского районного суда г. Екатеринбурга// [Электронный ресурс].URL:https://sud-praktika.ru/precedent/420329.html/(дата обращения 19.05.2021).
4. Приговор суда № 1-613/2017 по обвинению Мельниченко Н.П. по ч. 2 ст. 272 УК РФ / архив Октябрьского районного суда г. Ростова-на-ДонуURL:https://sud-praktika.ru/precedent/467627.html / (дата обращения 19.05.2021).
5. Приговор суда № 1-926/2017 по обвинению Семёнова Е.В. по ч. 1 ст. 273 УК РФ / архив Ленинский районный суд г. НовосибирскаURL: https://sud-praktika.ru/precedent/456303.html/ (дата обращения 19.05.2021).