[**Противодействие киберпреступности как фактор обеспечения экономической безопасности государства**](https://a24.biz/order/getoneorder/8128407)

**Диплом**

СОДЕРЖАНИЕ

ВВЕДЕНИЕ…………………………………………………………………………..…3

ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПРЕСТУПНОСТИ…………………………………………………...7

1.1. Киберпреступления: сущность, причины, последствия………………………...7

1.2. Выявление, предупреждение и профилактика киберпреступлений органами внутренних дел………………………………………………………………………..18

ГЛАВА 2. АНАЛИЗ НАПРАВЛЕНИЙ ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ…..20

2.1. Анализ методики выявления органами внутренних дел киберпреступлений..20

2.2. Анализ предупреждения и профилактики киберпреступлений……………….31

ГЛАВА 3. ПУТИ СОВЕРШЕНСТВОВАНИЯ ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ…..36

3.1. Совершенствование методики выявления органами внутренних дел киберпреступлений……………………………………………………………………36

3.2. Повышение эффективности комплекса мероприятий, проводимых в органах внутренних дел, по противодействию и профилактике киберпреступлений……..48

ЗАКЛЮЧЕНИЕ………………………………………………………………………..60

список использованных источников…………………………….63

[**Написание на заказ курсовых, дипломов, диссертаций...**](http://учебники.информ2000.рф/napisat-diplom.shtml)

**Вернуться в каталог готовых дипломов и магистерских диссертаций –**

[**http://учебники.информ2000.рф/diplom.shtml**](http://учебники.информ2000.рф/diplom.shtml)

ВВЕДЕНИЕ

**Актуальность темы исследования**. Интернет охватывает нашу жизнь каждый день. В связи с этим участились так называемые киберпреступления, совершаемые с помощью информационных технологий. С каждым годом преступники становятся все более изощренными и совершают «умные» преступления, требующие определенных навыков и способностей~~.~~ Это стало актуальным во время пандемии коронавируса, когда по меньшей мере четверть населения мира была вынуждена оставаться дома. Однако, уровень преступности не снизился, а в некоторых странах даже вырос. Это особенно касается киберпреступлений, совершенных с использованием информационных технологий.

Благодаря стремительному развитию информационных технологий были существенно упрощены и ускорены процессы обмена, поиска и сбора информации, что кроме положительных последствий обусловило появление качественно нового вида преступности – киберпреступности.

Проблема киберпреступности приобрела глобальный масштаб, а ущерб от нее достигает сотни миллиардов долларов. Сегодня киберпреступность становится все более распространенной, и связанный с ней незаконный финансовый оборот достигает триллионов долларов. В связи с этим задачи обеспечения информационной безопасности и кибербезопасности являются одними из наиболее важных для ведущих мировых держав.

Россия не стоит в стороне от проблем киберпреступности, уровень которой постоянно растет.

Для России данный вид преступлений является сравнительно новым, о чем также свидетельствует сравнительно-правовой анализ действующих в этой сфере нормативно-правовых актов.

Для нашего государства опасность киберпреступности носит двойной характер: с одной стороны в стране растет количество киберпреступлений, а с другой – российские хакеры все чаще стоят за крупнейшими мировыми киберпреступлениями.

В большинстве случаев, такая деятельность носит организованный характер. Вместе с тем, сформирована система противодействия киберпреступности относительно молода и нуждается не только в наполнении профессионалами но и формировании действенных механизмов сотрудничества как в стране, так и с иностранными партнерами. Дальнейшее ее развитие и профессиональное кадровое наполнение должно происходить именно с учетом организованного и транснационального характера киберпреступности.

Вышеизложенное обуславливает актуальность и особую значимость темы исследования.

Высокая социальная опасность таких преступлений вытекает и из их транснационального характера, так как последствия подобных деяний могут охватывать неограниченный круг лиц в самых разных странах. Преступник, объект преступного посягательства и потерпевший могут находиться на территориях разных государств.

При выявлении и расследовании киберпреступности знание работниками правоохранительных органов только уголовного и уголовно-процессуального законодательства, общих правил сбора доказательств является недостаточными. Поэтому, требуется не только особая тактика производства следственных действий и организационных мероприятий, но и, прежде всего, наличие специальных знаний в области компьютерной техники и программного обеспечения.

**Объектом** исследования является деятельность правоохранительных органов по расследованию киберпреступности.

**Предметом** исследования служит противодействие киберпреступности как фактору обеспечения экономической безопасности государства.

**Цель и задачи исследования**. Целью работы является комплексное исследование теоретических и практических проблем противодействия киберпреступности как фактору обеспечения экономической безопасности государства.

Для достижения цели были поставлены следующие **задачи**:

* выявить сущность, причины, последствия киберпреступления;
* рассмотреть выявление, предупреждение и профилактика киберпреступлений органами внутренних дел;
* проанализировать направления деятельности органов внутренних дел по противодействию киберпреступности;
* предложить пути совершенствования деятельности органов внутренних дел по противодействию киберпреступности.

**Степень научной разработанности проблемы**.

Теоретическую основу настоящего исследования составили труды следующих ученых: Гаджиев М.С., Зубова М. А., Коломинов В.В., Мтяйло Н.Э., Рахимова У.Х., Самурханов М.С., Сверчков В.В., Суслопаров А.В., Тропина Т.Л. и др.

Нормативно-правовую основу исследования составили: международно-правовые акты, Конституция РФ, российское уголовное законодательство, нормативно-правовые акты федеральных, региональных органов власти; научная литература, в которой анализируются и комментируются законодательство и законопроекты, правоохранительная деятельность.

Теоретическая значимость работы определяется тем, что в ней рассмотрены теоретические основы и научные концепции исследования киберпреступности.

Практическая значимость исследования определяется возможностью использования предложений и выводов для дальнейшей разработки теоретических проблем по противодействию киберпреступности.

Методологическая основа исследования. В работе применялись общенаучные и частонаучные методы исследования позволяющие получить новые теоретические сведения об объектах и предметах исследований.

**Структура работы** отвечает основной цели и предмету исследования. Работа состоит из введения, трех глав, заключения и списка использованных источников.

ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПРЕСТУПНОСТИ

1.1. Киберпреступления: сущность, причины, последствия

В начале необходимо выделить такое понятие, как «кибербезопасность».

Кибербезопасность (англ. – cybersecurity) – это сочетание людей, политик, процессов и технологий, используемых предприятием для защиты своих киберактивов. Кибербезопасность оптимизирована до уровней, определяемых бизнес-процессами компании, уравновешиванием требуемых ресурсов с удобством использования (управляемостью) и степенью компенсации риска. Подмножества кибербезопасности включают ИТ-безопасность, безопасность Интернета вещей (IoT), информационную безопасность и безопасность операционных технологий (ОТ).

Тезаурус кибербезопасности интегрирован с понятиями информационной безопасности, безопасности приложений, сетевой безопасности, безопасности Интернет, а также безопасности критической информационной инфраструктуры. По аналогии с классическим определением информационной безопасности в стандарте под кибербезопасностью фактически понимают свойство защищенности активов от угроз триады безопасности – конфиденциальности, целостности и доступности, но в некоторых абстрактных рамках – киберпространстве[[1]](#footnote-1).

Киберпреступления чаще совершаются в экономических целях. Это может быть, например, причинение экономического ущерба в виде кражи. Другие типы целей включают политические цели – нанесение ущерба основным государственным и политическим институтам, подрыв системы властных отношений и доверия к власти. Третий тип идеологических целей: распространение идей и идеологий с целью вербовки пользователей Интернета в ряды, например, радикальных террористических и националистических групп. Четвертый тип целей включает социально-психологические цели, такие как причинение морального, психологического вреда гражданам.

С появлением новых технологий, усовершенствованием Интранет-провайдингов, каждый человек все больше погружается в виртуальную среду, что означает следующее: чем больше новых возможностей, тем больше вероятность того, что каждый из нас может столкнуться с новыми проблемами, в частности, с Интранет-мошенничеством.

Зарубежные и отечественные ученые расходятся во мнениях относительно названия данного вида преступлений. В науке и законодательстве в разных странах существуют такие названия, как «преступления в области безопасности оборота компьютерной информации», «компьютерные преступления», «информационные преступления», «преступления в области высоких технологий», «киберпреступность» и др.

Одной из первых попыток определить термины, используемые в этой области, было Соглашение о сотрудничестве государств-членов Содружество Независимых Государства в борьбе с преступлениями в сфере компьютерной информации, подписанные еще в 2001 году в Минске. Согласно ст.1 указанного документа «преступления в сфере компьютерной информации» является уголовным преступлением, предметом посягательства на которое является компьютерная информация[[2]](#footnote-2).

Под киберпреступностью понимают совокупность преступлений, совершаемых в виртуальном пространстве с помощью компьютерных систем или путем использования компьютерных сетей и других средств доступа к виртуальному пространству, в пределах компьютерных сетей, а также против компьютерных систем, компьютерных сетей и компьютерных данных[[3]](#footnote-3).

В научной литературе также даются различные понятия киберпреступности (табл.1).

Таблица 1 – Определение понятия «киберпреступность»

|  |  |
| --- | --- |
| Автор | Определение |
| Зубова М.А. | совершенные виновно общественно опасные деяния, которые посягают на нормальный порядок обращения компьютерной информации, охраняемой законом, запрещенные под угрозой наказания УК РФ[[4]](#footnote-4). |
| Суслопаров А.В. | противоправные общественно опасные деяния, которые имеют свой дополнительный родовой объект – общественные отношения, направленные на обеспечение информационной безопасности общества. Они посягают на нормальный режим передачи, обработки и хранения данных в компьютерных системах (компьютерах)[[5]](#footnote-5). |
| Сверчков В.В. | неосторожные либо умышленные общественно опасные деяния (бездействие либо действия), которые предусмотрены статьями 272-274 главы 28 УК РФ. Они направлены против безопасности компьютерной информации, а также причиняют либо способны причинить вред благам, охраняемым законом (правам личности, отношениям собственности и т.п.)[[6]](#footnote-6). |
| Тропина Т.Л. | Совокупность преступлений, которые совершаются в киберпространстве посредством либо при помощи компьютерных сетей либо компьютерных систем, а также других средств доступа к киберпространству в рамках компьютерных сетей либо систем, против компьютерных данных, компьютерных сетей либо компьютерных систем[[7]](#footnote-7). |
| Самурханов М.С. | Совокупность преступлений, совершаемых в киберпространстве с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству, в рамках компьютерных систем или сетей, и против компьютерных систем, компьютерных сетей и компьютерных данных[[8]](#footnote-8). |

Один из известных подходов заключается в определении киберпреступлений как деяний, посягающих исключительно на безопасность компьютерной информации[[9]](#footnote-9).

Киберпреступность в более широком смысле – это любое противозаконное поведение, осуществляемое посредством или в связи с компьютерной системой или сетью, включая такие преступления, как незаконное владение, предложение или распространение информации посредством компьютерной системы или сети[[10]](#footnote-10).

Необходимо отметить, что источниками компьютерной информации являются системы (рис.1).

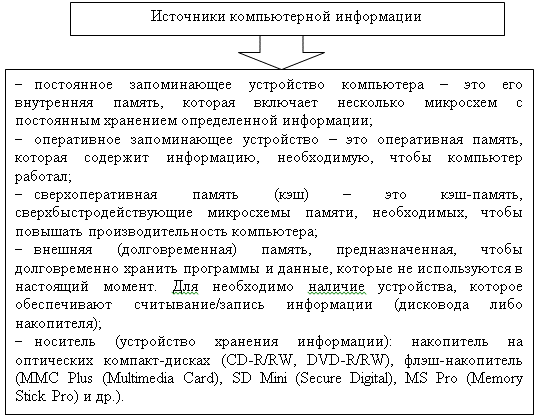


Рисунок 1 – Источники компьютерной информации

Непосредственным объектом киберпреступлений в сфере компьютерной информации является часть информационных отношений, непосредственно связанных с операциями над компьютерной информацией, в частности общественные отношения по соблюдению и обеспечению требований безопасности, законных способов получения, обработки и использования компьютерной информации, а также нормального функционирования компьютерной техники.

Также в качестве объекта киберпреступлений авторы выделяют следующий (табл.2).

Таблица 2 – Подходы к определению объекта киберпреступлений

|  |  |
| --- | --- |
| Автор | Объект киберпреступлений |
| Сафонов О.М. | Совокупность общественных отношений в сфере информационной безопасности, связанных с реализацией прав собственника или иного законного владельца компьютерной информации по реализации своих полномочий в отношении данной информации, и защите ее от неправомерного воздействия[[11]](#footnote-11). |
| Гузеева О.С. | Общественные отношения, обеспечивающие правомерный доступ, создание, хранение, модификацию, использование компьютерной информации самим создателем, потребление ее иными пользователями[[12]](#footnote-12). |
| Ефремова М.А. | Общественные отношения, обеспечивающие безопасность процессов хранения, обработки, предоставления информации посредством средств вычислительной техники и информационно-телекоммуникационных сетей[[13]](#footnote-13). |

Выделяют следующие признаки киберпреступности[[14]](#footnote-14):

1. Эти преступления совершаются в виртуальном пространстве или в рамках компьютерных сетей. Виртуальное пространство – это моделированное с помощью компьютера информационное пространство, в котором содержатся данные о лицах, явлениях, фактах, процессах, представленных в символьном, математическом либо ином виде. Такие сведения находятся в процессе движения по локальным и глобальным компьютерным сетям, хранятся в памяти любого виртуального либо физического устройства, специально предназначенных для их хранения, передачи и переработки.

2. Киберпреступления совершаются с помощью компьютерных систем или путем использования компьютерных сетей и других средств доступа к виртуальному пространству, а также против компьютерных систем, компьютерных сетей и компьютерных данных.

Наиболее распространенной является классификация киберпреступлений на агрессивные и неагрессивные.

К первой группе принадлежат: кибертерроризм, угроза физической расправы (например, переданная через электронную киберпреследование, киберсталкинг (противоправное сексуальное домогательство и преследование другого лица через Интернет), детская порнография (создание порнографических материалов, изготовленных с изображением детей, распространение этих материалов, получение доступа к ним).

Вторая группа включает: киберкража, кибервандализм, кибермошенничество, кибершпионаж, распространение спама и вирусных программ[[15]](#footnote-15).

Афанасьев и Репин в своей статье дают следующую краткую классификацию методов киберпреступлений и ИТ-инцидентов[[16]](#footnote-16):

1) незаконный доступ к информации;

2) утечка конфиденциальной информации;

3) удаление информации;

4) IT-мошенничество;

5) компрометация и саботаж информации;

6) аномальное поведение бизнес-приложений;

7) аномальная сетевая активность;

8) использование активов компании в личных целях либо в мошеннических операциях;

9) атаки типа «отказ в обслуживании» (DoS), включая распределенные атаки (DDoS);

10) подмена и перехват трафика;

11) фишинг, попытка взлома, взлом, сканирование портала компании;

12) сканирование сети, вирусные атаки, попытки взлома сетевых узлов;

13) анонимные письма (письма с угрозами);

14) размещение провокационной / конфиденциальной информации на блогах  и форумах.

Кибепреступления можно также разделить на следующие четыре основные группы (рис.2)[[17]](#footnote-17).

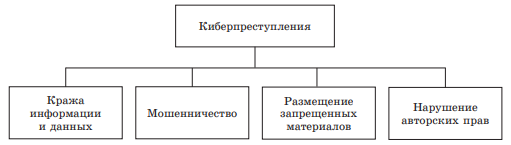


Рисунок 2 – Основные группы кибрпреступлений

Также выделяют классификацию киберпреступлений по различным признакам[[18]](#footnote-18):

1. По способу использования: компьютер является объектом правонарушения; компьютер используется как запоминающее устройство; компьютер используется как средство, способствующее совершению киберпреступления.

2. По наличию насилия: насильственные и иные потенциально опасные (кибертерроризм, угроза физической расправы, киберпреследование); ненасильственные (противоправное нарушение владения в киберпространстве, киберворовство, кибермошенничество, разрушение).

3. По способу воздействия: физические злоупотребления, операционные злоупотребления, программные злоупотребления, электронные злоупотребления.

Среди экономических причин киберпреступлений необходимо выделить следующие.

* монополизм разработчиков компьютерных программ, искусственное завышение цен на программные продукты. Также следует отметить, что постоянное изменение компьютерного программного обеспечения под видом его совершенствования приводит к перманентным внешне легальным тратам пользователей, которые при этом естественным образом пытаются сэкономить и ищут альтернативные способы решения возникающих проблем. Очевидно, что чаще всего эти альтернативные способы им предлагают киберпреступники;
* недобросовестная конкуренция вплоть до промышленного шпионажа между производителями программного обеспечения и антивирусной защиты. На практике происходит повсеместное нарушение авторских и патентных прав производителей программных продуктов и оригинальных технических решений, связанных с обеспечением компьютерных технологий и должной работы компьютерных сетей. При этом рядовой потребитель либо не может обнаружить подделку программного продукта, либо, что чаще всего, сознательно, как говорится, закрывает глаза на использование нелицензированной продукции, поскольку она заведомо дешевле оригинального продукта, а по своим качественным характеристикам нередко ничем ему не уступает;
* масштабное использование вредоносных компьютерных программ. Производители легального программного обеспечения, например, для затруднения деятельности конкурентов, а также чтобы привязать конкретных пользователей к своим программным продуктам, поскольку антивирусные программы также разрабатывают они, создают вредоносные программы;
* быстрое и относительно безопасное обогащение киберпреступников;
* максимальная незаконная прибыль, которую легко можно легализовать. Используя те же самые компьютерные технологии и тех же самых киберпреступников, которые совершали хищения денег, можно легализовать прибыль, что также удешевляет весь криминальный процесс.

В целом влияние киберпреступности на экономику отличается от воздействия иных форм противоправных действий[[19]](#footnote-19):

* киберпреступность негативно влияет на экономические системы самых разнообразных уровней (мировая экономика - национальная экономика - финансовая система и т.д.), нарушая связи между элементами данных систем. Объектом преступной деятельности в сфере информационных и телекоммуникационных технологий выступает информация. Ее хищение, изменение, неправомерное использование являются либо конечной целью, либо одной из промежуточных целей нарушителей закона. Таким образом, их деятельность прямо или косвенно направлена на нарушение стабильного функционирования информационных каналов в современных экономических системах. В настоящее время информация является одним из базовых экономических ресурсов. Условием успешного функционирования экономики выступают стабильное накопление, использование и обращение информации. Киберпреступность несет существенную угрозу для данных процессов;
* воздействие киберпреступности на экономику не носит выраженного институционального характера. Деятельность киберпреступников может быть индивидуальной, иррациональной, не подходящей под известные модели поведения. По этим причинам, а также в силу анонимности и интернациональности хакеры не формируют новые институты, способные взаимодействовать с формальными институтами, находить компромиссы;
* затраты ресурсов на реализацию преступного замысла хакерами могут быть на много порядков меньше, чем причиненный ими ущерб. В сфере киберпреступности даже один человек или небольшая группа злоумышленников могут причинить объекту кибератаки огромный ущерб.

Таким образом, киберпреступность носит ярко выраженный организованный характер, а в большинстве случаев и транснациональный, будучи чрезвычайно прибыльной сферой преступной деятельности. Электронно-вычислительная техника может выступать как средством совершения преступления, так и предметом преступления. Информация становится объектом преступлений: хищения, изменения или уничтожения путем несанкционированного доступа к ней. Киберпреступность содержит не только техническую и правовую, но и социальную проблему, эффективное решение которой требует, прежде всего, системного подхода к разработке основ обеспечения безопасности жизненно важных интересов гражданина, общества и государства в киберпространстве.

1.2. Выявление, предупреждение и профилактика киберпреступлений органами внутренних дел

Всегда сложно доказать киберпреступления из-за того, что данные типы преступлений имеют высокую латентность, и в большинстве случаев их трудно расследовать в силу многих объективных факторов, таких как[[20]](#footnote-20):

* некомпетентность сотрудников правоохранительных органов в области высоких технологий;
* нежелание жертв рассказать органам внутренних дел о преступлении.

Некоторые также отмечают сложность сохранения доказательной базы, поскольку чаще всего компьютерные преступления в сфере мошенничества совершаются крупными организациями.

Все преступления, как противоправные общественно опасные деяния, содержат нечто общее, и каждое отдельное преступление содержит те же основные правовые элементы, что и другие преступления.

Однако, исходя из характеристик киберпреступлений, можно сделать вывод, что этот список не является исчерпывающим. В этом случае должны быть установлены следующие обстоятельства[[21]](#footnote-21).

1) факт совершения преступного деяния, т.е. является ли данное действие или бездействие преступным;

2) предмет преступного посягательства – киберпреступность не ограничивается компьютерной информацией;

3) место совершения преступления – одно из важнейших условий, поскольку по статистике примерно 70% киберпреступлений пересекают национальные границы;

4) способ совершения преступления;

5) режим работы компьютерной системы или условия доступа к компьютерной информации, средствам защиты;

6) следы преступления. Обнаружение, фиксация и выемка следов преступления – одно из важных условий сбора необходимой доказательной базы;

7) характер и размер ущерба могут выражаться в имущественном, моральном и физическом ущербе, а также в нанесении ущерба деловой репутации;

8) личность лица, совершившего преступление. Установить это условие немного сложно из-за большой задержки киберпреступности;

9) условия и причины, способствовавшие совершению преступления.

Снижению рисков и последствий киберпреступлений способствует усиление кибербезопасности. Основной целью кибербезопасности является упрощение программ, управляющих киберрисками, чтобы любая фирма могла позволить внедрить ее у себя. Данные программы ориентированы на специфичные условия компании, ее потребности, склонность к риску и имеющиеся угрозы[[22]](#footnote-22).

Необходимо отметить, что наиболее уязвима для кибератак та категория граждан, которая пользуется компьютерами как дома, так и на работе, но при этом имеет слабое представление об основах кибербезопасности, а также электронных устройствах, направленных против компьютерных систем, компьютерных данных и компьютерных сетей.

Выявление, предупреждение и профилактика киберпреступлений происходит достаточно сложно, т.к. достаточно часто преступники прибегают к различному роду уловкам, маскируя свои преступные деяния разными по своей природе причинами, которые действительно могут иметь место быть (например, сбой в работе программного обеспечения, выход из строя носителя информации или какого-либо электронного устройства, несовершенство той или иной программы, т.н. «баги»).

Для выявления киберпреступлений, а также для установления лиц, занимающихся преступной деятельностью в этой области, создано Управление «К» – подразделение [Министерства внутренних дел России](https://ru.wikipedia.org/wiki/%D0%9C%D0%B8%D0%BD%D0%B8%D1%81%D1%82%D0%B5%D1%80%D1%81%D1%82%D0%B2%D0%BE_%D0%B2%D0%BD%D1%83%D1%82%D1%80%D0%B5%D0%BD%D0%BD%D0%B8%D1%85_%D0%B4%D0%B5%D0%BB_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B9%D1%81%D0%BA%D0%BE%D0%B9_%D0%A4%D0%B5%D0%B4%D0%B5%D1%80%D0%B0%D1%86%D0%B8%D0%B8), борющееся с [преступлениями в сфере информационных технологий](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%B5%D1%81%D1%82%D1%83%D0%BF%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%B2_%D1%81%D1%84%D0%B5%D1%80%D0%B5_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D1%8B%D1%85_%D1%82%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D0%B9)[[23]](#footnote-23).

Для киберпреступлений характерны такие ситуации[[24]](#footnote-24):

* собственник компьютерной системы обнаружил нарушение ее целостности и (или) конфиденциальности, установил виновное лицо и заявил о случившемся в правоохранительные органы;
* собственник самостоятельно выявил названные нарушения, однако не смог установить злоумышленника и заявил о случившемся;
* сведения о нарушении целостности и (или) конфиденциальности информации и виновном субъекте стали известны или обнаружены компетентным органом, владелец компьютерной системы этот факт скрывает.
* правоохранительным органом обнаружены признаки противоправного вторжения в компьютерную систему, виновное лицо и владелец информации неизвестны.

Таким образом, современная киберпреступность является не только результатом стремительного развития информационных технологий, но и важной и чрезвычайно прибыльной сферой преступной деятельности. Практически ни одно государство не стоит в стороне от данной проблемы. Направляя свои усилия на снижение рисков ее проявления на собственной территории, государства действуют в активном сотрудничестве, взаимопомощи и координации действий направленных на противодействие киберпреступности.

ГЛАВА 2. АНАЛИЗ НАПРАВЛЕНИЙ ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ

2.1. Анализ методики выявления органами внутренних дел киберпреступлений

Необходимо отметить, что с каждым годом, к сожалению, как в России, так и в мире наблюдается рост киберпреступности. Так, за 2015-2019 гг. количество киберпреступлений в России выросло более чем в 25 раз (с почти 11 тыс. в 2015 году до 295 тыс. в 2019). При этом динамика прироста преступлений в сфере информационных технологий за последние три года оценивается в 165% (в 2017 году их было совершено 66 тыс., в 2018-м – 175 тыс.). Преступления в киберпространстве отличаются высокой латентностью (раскрывается только одно из десяти). Случаи кибермошенничества в России практически не раскрываются, а их количество неуклонно растет (в 2019 году рост составил 40%)[[25]](#footnote-25).

В мировом масштабе киберпространство тоже не является полностью защищенным. Так, по официальным данным в 2019 году почти каждую четверть минуты осуществлялись атаки злоумышленников на информационные ресурсы во всем мире. По оценкам специалистов, к 2021 году частота зловредов увеличится и достигнет скорости почти каждой пятой доли минуты. Интересно что за 2019 год во всемирную паутину просочилось более 14 млрд. записей, содержащих конфиденциальную информацию. При этом в России наблюдался резкий скачок общего количества несанкционированного доступа (НСД) к информации (более, чем на 40%), в то время как в мировом масштабе он составил лишь 10% по сравнению с предыдущим периодом.

В число самых привлекательных для кибермошенников отраслей вошли производственная сфера, гостиничные, рекреационные услуги, услуги ремонта, финансовый сектор, страхование и недвижимость. По некоторым данным, индивидуальные киберпреступники могут зарабатывать в год до полумиллиона долларов США просто торгуя украденными данными (рис. 3)[[26]](#footnote-26).

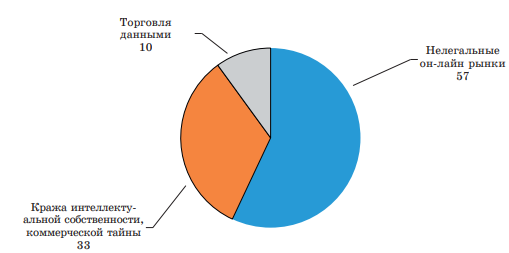


Рисунок 3 – Структура мирового рынка киберпреступлений, %

Способы злоумышленников становятся все изощреннее. Более половины мошенничеств в киберпространстве совершается во всемирной сети Интернет, более трети – с помощью средств мобильной связи, каждый десятый – с использованием банковских карт. Как показывает практика, около 80% пострадавших от киберпреступлений несут небольшой ущерб – менее 5 тыс. рублей. Как правило, один из пяти потерпевших не заявляет о произошедшем в полицию. Однако, ужасает их количество: по оценкам специалистов, число попыток совершения преступления может достигать 200–300 млн. в год. При этом 99% атак отсекаются автоматически аппаратно-программными сервисами.

Точной статистики о потерях, которые несет государство от киберпреступников, не существует. По официальным данным, это 120–130 млрд. р. в год, по неофициальным данным — не менее 600 млрд р. Но в любом случае можно противостоять атакам преступников, совершенствуя не только правоохранительные и судебные системы, но и ИТ-инфраструктуру, модернизируя финансовые инструменты и повышая грамотность населения в борьбе с кибер-мошенничеством. Экономические потери от киберпреступлений с каждым годом только увеличиваются (Приложение 1)[[27]](#footnote-27).

Так, по опубликованным данным оценки экспертов выручка крупнейших отечественных игроков на рынке по итогам 2018 г. увеличилась на 8% и достигла 111,5 млрд. руб., немного превысив показатель рекордного 2016 г. (111 млрд. руб.). В пересчете на доллары США рост оказался не столь значительным (+1%, 1,78 млрд. долл.США). Эти показатели коррелируют с общей динамикой ИТ-отрасли: выручка крупнейших ИТ-компаний России в 2018 г. выросла на 11,2% в рублях или на 3,75% в пересчете на доллары. Динамика рейтинга крупнейших поставщиков средств обеспечения информационной безопасности представлена на рисунке 4[[28]](#footnote-28).

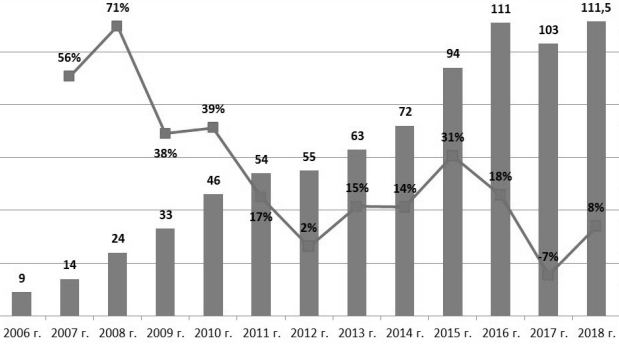


Рисунок 4 – Динамика рейтинга крупнейших поставщиков средств обеспечения информационной безопасности, млрд.руб.

Состав лидеров отрасли остался неизменным: пять ведущих компаний сохранили свои позиции (в соотношении с предшествующим периодом). К ним относятся «Лаборатория Касперского» (45,4 млрд.руб.), Softline (15,85 млрд.руб.), «Информзащита» (8 млрд.руб.), «ИнофТеКС» (4,5 млрд.руб.), а также «Инфосистемы Джет» (4,4 млрд.руб.) (рис. 5)[[29]](#footnote-29).



Рисунок 5 – Динамика рейтинга крупнейших поставщиков средств обеспечения информационной безопасности, млрд. долл. США

Лидерами по темпам роста выручки оказались разработчик ПО «С-Терра СиЭсПи» (+119%), а также интеграторы «Системный Софт» (+96%) и УЦСБ (+92%). Для компаний «Системный Софт» и УЦСБ взлет финансовых показателей был вызван завершением крупных проектов, которые были зафиксированы в отчетности по итогам года.

Рост выручки «Системного софта» связан с:

* реализацией ряда крупных проектов у ключевых заказчиков;
* расширением команды направления информационной безопасности, которая выросла до 12 человек.

Необходимо отметить, что киберугрозы развиваются ошеломительными темпами. По данным МВД России, в 2019 г. количество преступлений, совершенных с помощью IT-технологий, выросло почти на 70%. Почти половина из них (142,7 тыс.) относится к категориям тяжких и особо тяжких. В общем числе зарегистрированных удельных вес таких преступлений увеличился с 8,8 до 14,5%. Среди выявленных правоохранителями злодеяний традиционно преобладают кражи и мошенничества, совершаемые с помощью пластиковых карт, компьютеров и мобильников, подключенных к сети.

Киберпреступники и кибертеррористы постоянно берут на вооружение все новые практики, программные решения и технологические новации. Все это происходит на фоне революции в финансовом секторе, связанной с проникновением в финансовые технологии новых способов шифрования, транзакций и т.д. Неслучайно, по подсчетам Центра мониторинга и реагирования на компьютерные атаки в кредитнофинансовой сфере Банка России в 2019 г. мошенники провернули 576,5 тыс. операций с использованием электронных средств платежа без согласия клиентов банков – физических и юридических лиц, а общая сумма таких операций превысила 6,4 млрд. руб.[[30]](#footnote-30).

По официальным данным количество совершенных в России киберпреступлений за последние пять месяцев 2020 года превысило 180 тыс. Таким образом, данный показатель увеличился более чем на 85% по сравнению с аналогичным периодом прошлого года. Причиной такого резкого увеличения активности в киберпространстве послужила именно пандемия коронавируса[[31]](#footnote-31).

Отмечается стабильно высокий рост количества регистрируемых киберпреступлений в последние годы в России. В период с января по август 2020 года зарегистрировано 358,8 тысяч преступлений, что на 12,7% больше, чем за аналогичный период 2019 года (рис.6)[[32]](#footnote-32).

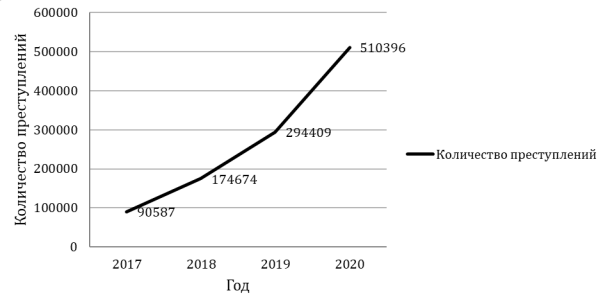


Рисунок 6 – Количество официально зарегистрированных преступлений в 2017–2020 гг., совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации

Более 461 тысячи киберпреступлений зафиксировано в России за 11 месяцев 2020 года, темпы роста количества таких преступлений в сравнении с итогами первого полугодия 2020 года замедлились с 91,7% до 76,6%. В России число киберпреступлений за январь 2021 года увеличилось на 32,2% по сравнению с аналогичным показателем прошлого года, следует из статистики МВД. Всего в первом месяце текущего года зарегистрировано 37,2 тыс. преступлений в области информационнотелекоммуникационных технологий. При этом рост количества преступлений, совершенных при помощи средств мобильной связи, составил 39%, а с использованием сети интернет – 51,3%[[33]](#footnote-33).

Помимо общего количества киберпреступлений, особого внимания заслуживает доля киберпреступлений среди всех зарегистрированных преступлений в России (рис.7)[[34]](#footnote-34).

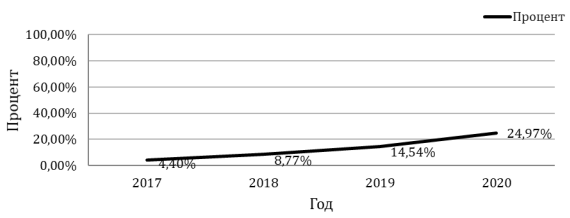


Рисунок 7 – Доля киберпреступлений по годам среди всех зарегистрированных преступлений в 2017–2020 гг., %

За 2017-2020 гг. произошел более чем пятикратный рост: в 2020 г. почти каждое четвертое преступление совершалось с использованием информационно-телекоммуникационных технологий. В 2021 г. стремительный рост доли преступлений продолжился и по состоянию на август 2021 г. составляет 26,5%.

В январе 2021 года доля преступлений в сфере высоких технологий от общего числа выросла до 25%, тогда как год за аналогичный период 2020 г. она составляла 17,7%.

В наиболее экономически развитых субъектах в январе–августе 2021 г. показатель приблизился к 40%36: в Москве — 39,7%, в Санкт-Петербурге — 38,9%. По всей видимости, сложившийся устойчивый тренд на увеличение доли киберпреступлений по всей стране в ближайшее время сохранится, а крупнейшие города России показывают «опережающее развитие» в данном процессе.

Наибольший прирост киберпреступлений в 2020 г. зарегистрирован в Северной Осетии, а также в Севастополе, Тульской и Ленинградской областях (рис.8)[[35]](#footnote-35).

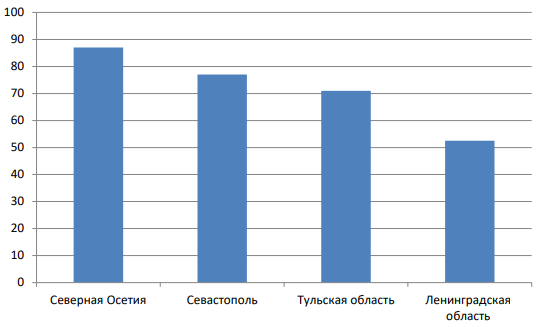


Рисунок 8 – Прирост киберпреступлений в 2020 г. (%)

Больше всего таких преступлений выявили в Москве, Мурманской области, Чувашии, Ханты-Мансийском и ЯмалоНенецком автономных округах.

Наименьший прирост зафиксирован в Ненецком автономном округе, Еврейской автономной области, Магаданской, Курганской и Смоленской областях. Меньше всего подобных преступлений было совершено в Чечне, Дагестане, Ингушетии, Туве и Подмосковье.

Самые распространенные киберпреступления – это (табл.3)[[36]](#footnote-36):

* неправомерный доступ к компьютерной информации;
* создание, использование и распространение вредоносных компьютерных программ;
* мошеннические действия, совершенные с использованием электронных средств платежа.

Таблица 3 – **Число киберпреступлений за 2016-2019 гг.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Вид преступления | 2016 г. | 2017 г. | 1 полугодие 2018 г. | 1 полугодие 2019 г. |
| Преступления в сфере компьютерной информации | 1748 | 1883 | 1192 | 1233 |
| Мошенничество с использованием электронных средств платежа | 266 | 228 | 110 | 741 |
| Неправомерный доступ к компьютерной информации | 994 | 1079 | 722 | 827 |
| Создание, использование и распространение вредоносных компьютерных программ | 751 | 802 | 470 | 406 |
| Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей | 3 | 2 | 0 | 0 |

Одна из самых важных характеристик киберпреступности в России – это низкий процент раскрываемости (рис.9)[[37]](#footnote-37).

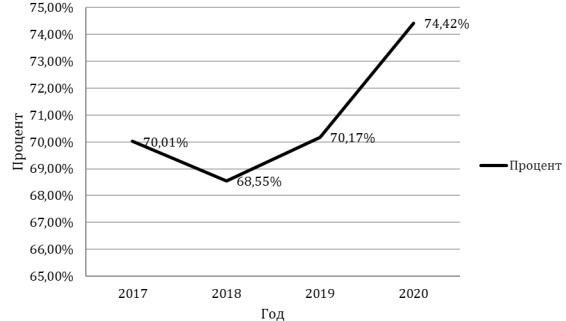


Рисунок 9 – Доля нераскрытых киберпреступлений относительно всех зарегистрированных преступлений в 2017–2020 гг.

Доля нераскрытых киберпреступлений не только остается на стабильно высоком уровне — в районе 70%, но и показывает небольшой рост в 2017-2020 гг., несмотря на активную деятельность российских государственных органов и организаций, особенно банковского сектора.

В 2018 г. число мошенничеств при использовании платежных карт увеличилось в 7 раз. Раскрываемость киберпреступлений в данной сфере колеблется ежегодно от 45 до 53 процентов (рис.10) [[38]](#footnote-38).

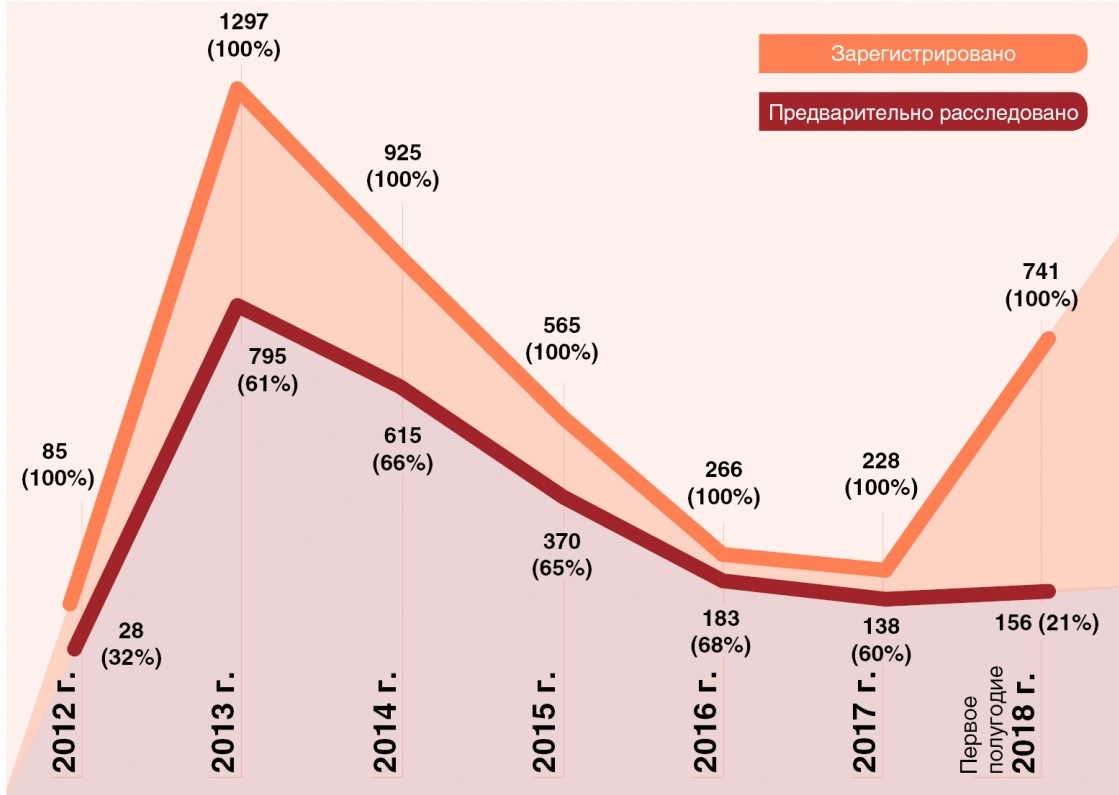


Рисунок 10 – Количество мошенничеств при использовании платежных карт за 2012-2018 гг.

Количество расследованных киберпреступлений уменьшилось в 2018 г. на 19,6%. В 2018 г. количество выросло на 30,5% количество нераскрытых киберпреступлений. Общая же раскрываемость в 2018 г. составила 41,3%. (табл.4)[[39]](#footnote-39).

Таблица 4 – Расследованные и нераскрытые киберпреступления в 2017-2018 гг.

|  |  |  |
| --- | --- | --- |
|  | 2017 г. | 2018 г. |
| Расследовано | 903 | 726 |
| Число нераскрытых | 790 | 1031 |

Следует отметить, что от 70% до 80% киберпреступлений не были заявлены потерпевшими, а от 30% до 20% были укрыты. Главным фактором гиперлатентности, пожалуй, выступает вы­сокий уровень терпимости самих потерпевших, которые или пыта­ются решить проблему утраты данных альтернативными способами (к примеру, обращаясь за восстановлением аккаунта непосредственно к администраторам интернет-ресурса), или не спешат заявлять об этом в полицию, поскольку не желают тратить собственное время на разбирательство, не верят в возможности правоохранительных ор­ганов по поимке злоумышленников, не желают огласки каких-либо компрометирующих сведений при исследовании предшествующей виртуальной активности самого потерпевшего в сети Интернет и др.

Таким образом, на текущий момент киберпреступление является одной из самых быстро растущих категорий преступлений в России. Развитие киберпреступности идет в ногу с развитием информационно-технических средств, а мотивы киберпреступников также видоизменяются с развитием таких преступлений. Кибератаки стали массовым явлением, а их направления задевают все сферы общества.

Стоит констатировать, что предпосылки зарождения и развития киберпреступности формировались в России в течение последних нескольких лет. Во-первых, это цифровизация различных сторон жизнедеятельности россиян: например, высокий интерес к банковским картам и счетам, безналичным способам оплаты, онлайн-досуг и активное использование соцсетей. Во-вторых, сохраняющийся низкий уровень цифровых компетенций граждан страны. В-третьих, низкая квалификация правоохранительных органов, несовершенство антифрод-инфраструктуры, неспособность оперативно пресекать киберпреступную деятельность и эффективно расследовать инциденты в цифровой среде.

2.2. Анализ предупреждения и профилактики киберпреступлений

В современных условиях, как правило, защиту информации обеспечивают при помощи:

– установки фильтра (причем это может быть аппаратное средство – например, экран, либо программа-блокиратор сигналов);

– контроля за действиями в пределах охраняемой ИС;

– кодирования информации;

– четкого разграничения прав доступа, – комплексного подхода к обеспечению информационной безопасности защищаемых ресурсов.

В настоящее время одним из основных способов обеспечения информационной безопасности в России является антивирусная программа – 99%. Кроме этого, можно отметить средства администрирования и NGFW (Firewall и Proxy) – 87 и 63%, соответственно.

В странах СНГ также основным методом защиты информации является антивирусная программа, но процент использования несколько меньше – 97%. Средства администрирования отмечаются в 71%, NGFW (Firewall и Proxy) – несколько выше, чем в России – 64%.

Положительным фактом является то, что руководители предприятий и организаций стали больше внимания уделять обеспечению информационной безопасности. Компании наиболее часто используют средства обеспечения информационной безопасности, такие как DLP-системы (Data Leak Prevention – «предотвращение утечек данных») – это программное обеспечение, защищающее информационные ресурсы компании от утечек конфиденциальной информации. Они создают защищенный цифровой «периметр» вокруг организации, анализируя всю исходящую и входящую информацию (причем не только передаваемую по каналам связи в электронном виде, но и посредством других информационных потоков). Данная система снабжена встроенными механизмами определения степени конфиденциальности любого обнаруженного в перехваченном трафике документа, как правило, путем анализа его содержимого.

Кроме предупреждения проблемы НСД к информации эти программные продукты осуществляют решение сопутствующих проблем (начиная с аудита использования рабочего времени и ресурсов организации до контроля правомерности действий сотрудников и даже мониторинга общения работников между собой с целью выявления проблемных тем, наносящих вред компании). Проблема лишь состоит в необходимости подготовки квалифицированных специалистов для эффективной работы данной системы, что, несомненно, влечет дополнительные расходы[[40]](#footnote-40).

Прямо сейчас мы наблюдаем мощную волну цифровизации преступной деятельности, активное использование технологий при совершении противоправных действий. Перечислим ключевые факторы, которые, способствовали возникновению негативной ситуации с состоянием киберпреступности в России[[41]](#footnote-41):

* дисбаланс между темпами цифровизации в России и ростом уровня цифровых компетенций граждан страны. Масштабы цифровизации в России велики: например, на 2020 г. пришелся рекорд по количеству выданных банковских карт, активное использование безналичных способов оплаты, рост аудитории соцсетей и их активности. Наряду с этим сохраняется низкий уровень компетенций россиян в сфере цифровых технологий: с 2019 г. остается неизменным количество россиян с продвинутым уровнем цифровых компетенций – 27%. Многие граждане до сих пор обладают недостаточными знаниями и навыками в сфере информационных технологий, необходимыми для безопасного использования цифровых продуктов.

Стоит оговориться, что высокий уровень цифровых компетенций не гарантирует полную защиту от киберпреступников, особенно использующих методы социальной инженерии, однако снижает вероятность стать жертвой мошенников. На текущий момент сложилась ситуация, когда многие граждане вынужденно или добровольно пользуются цифровыми продуктами, не имея для этого достаточного уровня знаний и навыков. Такие обстоятельства – благодатная почва для роста кибермошенничества. Например, по состоянию на 2021 г. более 70% пенсионеров в России получают выплаты на банковские карты. Пожилые люди – это один из наиболее уязвимых слоев населения, что подтверждается исследованиями: например, пожилой возраст положительно связан с общим уровнем доверия, в том числе и к незнакомцам. Данной особенностью пожилых людей нередко пользуются мошенники, эксплуатируя доверие людей преклонного возраста и совершая в отношении них финансовые преступления. В течение пандемии пенсионерам и семьям с детьми периодически производились единовременные массовые выплаты от государства, что также привлекало внимание мошенников.

Часто и сами граждане создают благоприятные условия для совершения в отношении них киберпреступлений, разглашая личную информацию в соцсетях, которой эффективно пользуются преступники, которые совершают действия по распространению вирусов, финансовому мошенничеству, краже аккаунтов. Особенно часто стали применяться методы социальной инженерии, которые показывают высочайший уровень эффективности, принуждая человека совершать порой абсолютно абсурдные вещи, например, выбрасывать собственные сбережения в окно. Неудивительно, что преступления с использованием методов социальной инженерии рассматриваются как серьезная угроза безопасности не только отдельно взятого человека, но и информационных сетей различных организаций. Факты свидетельствуют о том, что в обозримом будущем именно такого рода преступления будут наиболее распространенными среди всех видов киберпреступлений;

* недостаточный уровень эффективности в противодействия киберпреступной деятельности: низкий уровень компетенций со стороны правоохранительных органов, несовершенство антифрод-инфраструктуры. Проблема подчеркивается в том числе и высшим руководством правоохранительных органов. Правоохранительные органы отстают от киберпреступников в техническом обеспечении и инструментах связи. Следствием недостаточного уровня компетенций правоохранительных органов становится низкий процент раскрываемости киберпреступлений, который продолжает снижаться в последние несколько лет. Ежегодно практически удваивалось количество совершаемых киберпреступлений в России в 2018 и 2019 гг., а их доля среди всех преступлений с 2017 по 2019 гг. увеличилась в 3,3 раза. Тем не менее, активных действий со стороны властей в допандемийный период не предпринималось: например, еще в 2015 г. была направлена инициатива о создании подразделения МВД по борьбе с преступлениями в соцсетях, в 2019 г. Владимир Путин усомнился в необходимости создания киберполиции. В 2021 г. президент уже констатировал проблему с раскрываемостью киберпреступлений в стране. Помимо низкой раскрываемости, существуют проблемы со скоростью реагирования на активность кибермошенников. Так, на Прямой линии с Владимиром Путиным в 2021 г. президент отметил, что сейчас на блокировку мошеннических фишинговых сайтов уходит до трех дней, хотя ранее уходили недели или даже месяцы.
* фишинг – это попытка обманом заставить клиентов раскрыть свою личную информацию о безопасности; номера их кредитных карт, данные банковского счета или другую конфиденциальную информацию, выдавая себя за заслуживающие доверия компании в электронном письме.

Одна из особенностей фишинга – это его хорошая масштабируемость, и деятельность мошеннического сайта даже в течение нескольких минут может нанести значительный урон. Защита граждан от фишинговых сайтов – важный аспект информационной безопасности, и стоит констатировать, что на текущий момент скорость реакции российских правоохранительных органов на такого рода преступную активность все еще недостаточно оперативная, несмотря на положительную динамику.

Таким образом, несколько лет назад был не замечен или проигнорирован тренд на зарождение новой масштабной социальной проблемы в России – киберпреступности. Было упущено время на работу с населением, подготовку инфраструктуры, соответствующих подразделений, налаживание международного сотрудничества и выстраивание законодательной базы. Сейчас можно наблюдать поспешные действия в попытке исправить ситуацию, которая становится все более критической: создание в МВД РФ и Следственном комитете подразделений по борьбе с киберпреступностью, работа по информированию граждан о новых видах мошеннических схем, запуск специальной платформы для борьбы с мошенничеством, международное сотрудничество на высочайшем уровне, технологии по определению телефонных мошенников со стороны банковского сектора. Тем не менее сторона противодействия преступной деятельности в данном противостоянии занимает на текущий момент отстающую позицию: количество киберпреступлений продолжает расти.

ГЛАВА 3. ПУТИ СОВЕРШЕНСТВОВАНИЯ ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ

3.1. Совершенствование методики выявления органами внутренних дел киберпреступлений

Проблемы в выявлении и расследовании преступлений в сфере компьютерной информации можно было условно разделить на организационные и правовые. Так же можно было бы еще выделить смешанные – «организационно-правовые», но так или иначе все проблемы тесно связаны между собой[[42]](#footnote-42).

Правовые проблемы являются весьма актуальными. Именно от них зависит возможность решения организационных проблем.

Правовой вакуум не позволяет дать правильную оценку совершенным деяниям, что приводит правоохранительные органы и суд к неоднозначной оценке совершенных деяний. То есть к сомнениям.

Основные понятия в законах были сформулированы более 30 лет назад, то есть в прошлом веке. За это время научно-технический прогресс шагнул так далеко, что впору отменять все ранее принятые законы и принимать принципиально новые. Тот же Spam, который оценивается законодательством многих стран как преступление в сети Интернет, никаким образом не регулируется на федеральном уровне в России. В своей практике неоднократно приходилось сталкиваться с данной проблемой, когда не только простых граждан, но и администраторов компьютерных сетей закидывали спамом так, что почтовые сервера отказывали в обслуживании.

Возникающие в борьбе с преступлениями компьютерной информации проблемы, обусловлены несовершенством уголовно-правовых норм, противоречивостью их толкования, отсутствием научно-методических рекомендаций и официальных руководящих разъяснений по квалификации этих деяний, например, постановлений Пленума Верховного суда РФ, а также ратифицированных международных договоров и соглашений по эффективной совместной борьбе с данными видами преступлений[[43]](#footnote-43).

В Российском законодательстве до сих пор отсутствует четкий понятийный аппарат, касающийся информации и информационного обмена. Это дает в свою очередь, возможность манипулировать понятиями, вводить в заблуждение суд и уходить от ответственности. Если рассматривать подробнее нормативно-правовые акты РФ, то видно явное расхождение в понятиях и отсутствие четких определений, особенно в научных понятиях и технических терминах в нормативно-правовых актах, ГОСТах и Технической литературе.

Поэтому в субъектах РФ правоохранительные органы, осуществляющие борьбу с преступлениями в сфере компьютерной информации, вынуждены собирать для судов и следствия своеобразные мини-методички и заверенные отдельные разъяснения специалистов, в которых в доступной форме для неподготовленного человека разъясняются термины, способы защиты информации в ЭВМ и т.д.

В Российской Федерации действует сегодня более ста нормативных правовых актов различного уровня, касающихся вопросов формирования различных видов общедоступных информационных ресурсов и обеспечения доступа пользователей к открытой информации. Тем не менее, понятие доступа к информации законодательно не закреплено, субъекты и объекты доступа в различных нормативных правовых актах определяются по-разному, механизмы доступа к информации также не определены.

Понятие «доступ к информации» многогранно и многоаспектно, в связи с чем, его разработка, соотношение доступа к информации и ее доступности как качественной характеристики, состояния, свойства информации, информационных систем, а также их единообразное восприятие требуют соответствующего законодательного урегулирования, которое позволит закрепить механизм реализации прав на доступ к информации. Это необходимо закрепить в Федеральном законе «О персональных данных». Можно отметить, что в соответствии с теорией криминалистики, следы бывают двух типов – материальные и идеальные. Исходя из этого, можно поставить под сомнение понятие копирования компьютерной информации, если злоумышленник зрительно скопировал ее себе в память (в мозг), ведь законодатель преследует лишь копирование информации на машинные носители (а не на бумажные или фото, например).

Требуется разграничение в законодательстве различных видов конфиденциальной информации, а также установление режимов их защиты, в том числе в телекоммуникационных сетях, для чего необходима разработка Федерального закона «О конфиденциальной информации», в котором должны получить отражение вопросы защиты указанной информации. Этот закон особенно актуален в связи с участившимися случаями преступного использования персонифицированной информации обо всех аспектах личной жизни каждого человека. Пример - хищение и распространение баз данных с личными данными населения и сотовых операторов и т.д. К сожалению, все эти базы не имеют соответствующего юридического статуса, потому что до сих пор не принят федерального закона «Об информации персонального характера», предусматривающего механизмы контроля за использованием персональных данных и ответственность за неправомерное их использование. Хотя делались попытки приравнять эти базы к коммерческой информации, но безуспешно[[44]](#footnote-44).

Этот вид преступности непосредственно затрагивает сферу информационной безопасности личности и напрямую связан с угрозой нарушения прав человека через информационную сферу.

Еще в 2001 году Межведомственной комиссией Совета Безопасности Российской Федерации по информационной безопасности одобрены «Основные направления нормативного правового обеспечения информационной безопасности Российской Федерации», согласно которым в число первоочередных мер по совершенствованию нормативного правового обеспечения информационной безопасности включена разработка следующих законопроектов: «О персональных данных», «О праве на информацию», «О коммерческой тайне», «О неприкосновенности частной жизни, о личной и семейной тайне», «О защите нравственности», «О служебной тайне», «О национальной безопасности».

Почти аналогично стоит вопрос и со сбором доказательств. Одним из самых сложных вопросов, возникающих при выявлении и расследовании информационных преступлений: «можно ли полученную при обыске распечатку или информацию на магнитных носителях рассматривать как доказательство».

В Российском законодательстве электронный документ активно отнесен к документированной информации. Он определен как документ, в котором информация представлена в электронно-цифровой форме. Насчет доказательной силы такого документа сказано, что он может быть письменным доказательством при условии, если можно установить его истинность. То есть, возможность суда произвести определенную проверку или экспертизу – главный критерий допустимости подобных документов как доказательства в суде. Возникла необходимость в некотором «показателе подтверждения» истинности информации[[45]](#footnote-45).

На первый взгляд проблема была якобы решена с помощью системы электронной цифровой подписи, являющейся реквизитом электронного документа, который защищает его от подделки. Он получается в результате криптографического преобразования информации с использованием закрытого ключа, позволяющего идентифицировать собственника, а также устанавливает отсутствие искажения информации в электронном документе. Действие электронного документа, скрепленного электронной подписью, обусловлено наличием в автоматизированной информационной системе программно-технических средств, обеспечивающих идентификацию подписи, и соблюдением установленного режима его использования. Однако если таковых нет, то в доказательную базу его приобщать нельзя.

Эта же проблема относится и к сбору первичной проверочной информации при проведении первоначальных оперативно-розыскных мероприятий. Например, при сборе образцов для сравнительного исследования. Ведь, по сути, каждая программное или аппаратное средство, используемое при этом, должно быть сертифицировано. А это, порой, выполнить просто невозможно. Законодательно не закреплена и возможность наблюдения, по постановлению суда естественно, за поведением преступника в сети, фиксации его действий, особенно на территории других стран. И при получении каких-либо документальных подтверждений из этих стран, признании этих документов доказательствами.

Не урегулирован пока в полной мере, но уже имеет определенные перспективы, вопрос о предоставлении суду электронных копий традиционных документов (в том числе последовательности действий следователя, судьи и т.д. при просмотре, изъятии и фиксации доказательств без случайного внесения изменений).

Для того чтобы распечатку можно было признать доказательством, нужно, чтобы она снималась только с помощью специально паспортизованных программ, которые прошли соответствующий контроль на защиту от возможности внесения изменений в распечатываемую (или копируемую) информацию. При этом в уголовно-процессуальном законодательстве не определены процедуры проведения таких действий, как снятие копии с машинных носителей и распечатка информации[[46]](#footnote-46).

Открытым на сегодня остается и вопрос проведения экспертизы электронного документа. В соответствии с Законом Российской Федерации от 31.05.01 г. № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации» в системе МВД России функционирует Государственное учреждение «Экспертно-криминалистический центр (ЭКЦ) МВД России». В его структуре функционирует 18-й отдел «Компьютерных экспертиз и технологий», который специализируется на производстве относительно нового вида экспертных исследований, сформировавшихся вначале 90-х годов прошлого века и получивших официальное название «Судебная компьютерно-техническая экспертиза».

Налицо ситуация, когда существует Доктрина, Федеральные законы, но во многом отсутствует нормативная база, которая должна служить инструментом для воплощения этих законов.

Организационные особенности и проблемы в выявлении и расследовании преступлений в сфере компьютерной информации приводят к некорректному проведению оперативных мероприятий и следственных действий и потере значимой информации (в том числе и исключению из материалов уголовных дел собранной информации)[[47]](#footnote-47).

Их можно разделить на следующие:

* использование новейших информационных технологий, требующих специального образования и высокого интеллектуального уровня;
* высокий уровень латентности до 90%, обусловленный, в частности, совершением этого вида правонарушений в нематериальной сфере и, как правило, нежеланием жертв предоставлять об этом информацию;
* трудность подсчета материального ущерба от совершаемых преступлений (например, в Ульяновской области по уголовным делам при причинении материального ущерба путем неправомерного доступа к компьютерной информации, проводится бухгалтерская экспертиза, которая может точно подсчитать ущерб только по данным с аппаратуры АПУС ГТС и только по зарегистрированным соединениям), при этом сразу же возникает трудность в квалификации деяний;
* трудность сбора и закрепления доказательной информации (практически всегда на получение информации о преступлении требуется постановление суда);
* высокий рост данного вида преступлений из-за невозможности высококвалифицированных специалистов как-то прожить, и как следствие совершение ими «беловоротничковых» преступлений;
* возможность совершения преступлений с помощью средств удаленного доступа, что не требует от преступника присутствия на месте преступления (преступление совершается в одном месте земного шара, а последствия наступают в другом);
* активное сращивание с организованной преступностью;
* интернационализация данного вида преступлений;
* невозможность выработки каких-то стандартных методик по раскрытию преступлений – каждое новое техническое решение предполагает новый вид и способ совершения преступления[[48]](#footnote-48).

Из-за сложности понятийного аппарата, технической глубины проблемы, и часто, непонимания проблемы суды не рассматривают их как серьезную угрозу. С подачи средств массовой информации, обычный гражданин воспринимает киберпреступника как умную и интересную личность, который один борется с жадной и глупой жертвой, ловко ускользая от цепких рук правосудия. Поэтому пострадавшие от компьютерных преступлений не спешат выставлять себя на посмешище.

Как показывает практика, расследование компьютерных преступлений требует специальных знаний и практических навыков при проведении первоначальных следственных действий по таким делам. Сотрудник ОВД обязан обладать не только правовыми и криминалистическими навыками, но и разбираться в тонкостях работы компьютерных систем, т.е. быть специалистом и в области информационных технологий[[49]](#footnote-49).

Оперативный сотрудник ОВД, занимающийся выявлением и расследованием дел по компьютерным преступлениям, должен быть программистом или, по крайней мере, разбираться в нюансах использования и возможностях вычислительной техники. Сказываются также недостаточные знания работников правоохранительных органов в этой сфере отношений, и их высокая загруженность несвойственными функциями, и устанавливаемый режим работы только днем, когда основная часть преступлений совершается в ночное время, низкий уровень материально-технического оснащения, а также требования к широкой специализации сотрудников ОВД из-за недостатка кадров и штатной численности, в то время, когда преступники имеют узкую «специализацию» (хакеры, ньюкеры, кардеры, фрикеры, крекеры и т.д.), свободное время, часто бесплатный (за чужой счет) доступ в Интернет.

Следователи в субъектах РФ одновременно ведут дела и по общеуголовным делам, таким как тяжкие телесные повреждения, разбои, изнасилования и одновременно по преступлениям в сфере компьютерной информации, которые требуют специальных познаний. При отсутствии определенного опыта, следственной и судебной практики, законодательной поддержки следователи с неохотой берутся за расследование подобных дел. А при явном отсутствии международных норм и процедур сбора и закрепления доказательной базы в настоящее время не может идти и речи о каком-то быстром и эффективном расследовании преступлений в сфере компьютерной информации, совершенных в других странах, или из других стран[[50]](#footnote-50).

Исходя из рассмотренных проблем можно было бы попытаться определить возможные пути из решения. Общество само приходит к выводу, что доверие и безопасность относятся к главным опорам информационного общества. Исходя из правовых проблем в Российской Федерации необходимо скорейшее принятие законодательных актов, затрагивающих сферу высоких технологий, с учетом имеющейся статистики и судебной практики, внести поправки в уже действующие законы.

Для оказания эффективного противодействия этому виду преступлений усилий только на национальном уровне недостаточно. Необходима разработка, стандартизация и унификация законодательства и программных средств, позволяющего определять местонахождение и установление личности преступников, противоправно использующих компьютерные сети и глобальные телекоммуникационные системы, как это пытаются сделать страны подписавшие Европейскую конвенцию по борьбе с киберпреступностью.

Также хотелось акцентировать внимание на решении проблемы унификации законодательства стран, участвующих в информационном обмене. Без единых требований к доказательствам ни один суд ни одной страны не признает доказательством данные, если они будут собраны в другой стране по законам, противоречащим законам запрашивающей страны. Для этого необходимо уже сейчас провести анализ проблемы сопряжения национальных законодательств отдельных стран в части, регулирующей вопросы информационной безопасности, с тем, чтобы обеспечить унифицированную классификацию правонарушений в сфере информационной безопасности и ответственность, возникающую в связи с совершением действий, классифицируемых как преступные.

Необходимо заострить внимание на решении организационных проблем обнаружения и идентификации преступников в сфере компьютерной информации в международном масштабе с помощью оперативно-розыскных мероприятий. При этом, для признания судами различных стран в качестве доказательств документов, предусмотреть методы фиксации, сбора и передачи их потерпевшей стороне, возможности точного определения географического местоположения узлов сети Интернет для того, чтобы правоохранительные органы могли определить страну происхождения и тем самым страну процессуальной юрисдикции, в том числе используя компьютерную разведку. А для этого переработать уже существующие законы и принять новые, в том числе ратифицировать Европейскую конвенцию по киберпреступности.

Особую роль могла бы сыграть международная интегрированная база данных киберпреступников, в которой фиксировались лица, склонные к совершению преступлений в сфере компьютерной информации, криминалистическая характеристика совершенных преступлений и т.д. При этом необходимо разработать и внедрить легендированные закрытые каналы доступа в сеть между подразделениями киберполиции различных стран для повседневной и экстренной связи. Возможно, международные соглашения должны включать некоторые процессуальные санкции.

Выявление, раскрытие и расследование преступлений в сфере компьютерной информации происходит достаточно сложно, поскольку зачастую преступники прибегают к различному роду уловкам, маскируя свои преступные деяния разными по своей природе причинами, которые действительно могут иметь место быть (например, сбой в работе программного обеспечения, выход из строя носителя информации или какого-либо электронного устройства, несовершенство той или иной программы, т.н. «баги»).

Поэтому в процессе начального этапа расследования, возникают сложности. Определить умышленность совершенного деяния, установить признаки правонарушения, разграничить административные правонарушения от преступлений, разграничить составы совершенных преступных посягательств с учетом изменяющегося уголовного законодательства достаточно сложно без специальных знаний.

Для выявления преступлений в сфере компьютерной информации, а также для установления лиц, занимающихся преступной деятельностью в этой области, создано Управление «К» — подразделение [Министерства внутренних дел России](https://ru.wikipedia.org/wiki/%D0%9C%D0%B8%D0%BD%D0%B8%D1%81%D1%82%D0%B5%D1%80%D1%81%D1%82%D0%B2%D0%BE_%D0%B2%D0%BD%D1%83%D1%82%D1%80%D0%B5%D0%BD%D0%BD%D0%B8%D1%85_%D0%B4%D0%B5%D0%BB_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B9%D1%81%D0%BA%D0%BE%D0%B9_%D0%A4%D0%B5%D0%B4%D0%B5%D1%80%D0%B0%D1%86%D0%B8%D0%B8),[[51]](#footnote-51) борющееся с [преступлениями в сфере информационных технологий](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%B5%D1%81%D1%82%D1%83%D0%BF%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%B2_%D1%81%D1%84%D0%B5%D1%80%D0%B5_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D1%8B%D1%85_%D1%82%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D0%B9) (выявление и пресечение фактов неправомерного доступа к компьютерной информации; борьба с изготовлением, распространением и использованием вредоносных программ для ЭВМ; противодействие мошенническим действиям с использованием возможностей электронных платежных систем; борьба с распространением порнографических материалов с участием несовершеннолетних через сеть Интернет).

В любом случае, при получении следователем или иным уполномоченным на то лицом сообщения о совершении преступления в сфере компьютерной информации должна быть проведена, как правило, органами дознания, доследственная проверка.

При этом типичными являются следующие проверочные ситуации.

Пользователь информациии самостоятельно выявил нарушение целостности и конфиденциальности информации, обнаружил виновное лицо и заявил об этом в правоохранительные органы. Это дна из самых редких ситуаций, которая практически не встречается в практике в силу объективных причин.

Пользователь информации собственными силами выявил нарушение целостности и конфиденциальности информации в системе, не смог обнаружить виновное лицо и заявил об этом в правоохранительные органы.

Как показывает практика, наиболее сложные преступления в сфере компьютерной информации совершаются с использованием возможностей, предоставляемых глобальными компьютерными сетями. Поэтому при раскрытии и расследовании данных преступлений исследуются следы, которые создаются не только в технических средствах пользователя, но формируются в результате прохождения информации по самим техническим каналам связи.[[52]](#footnote-52)

Именно поэтому такая ситуация случается довольно часто, поскольку главная проблема при выявлении, раскрытии и расследовании компьютерных преступлений заключается в установлении личности преступника, так как специфика совершаемых преступлений и заключается в анонимности пользователей информационных технологий.

Еще одной типичной проверочной ситуацией является довольно распространенная обстановка, при которой данные о нарушении целостности и конфиденциальности информации в информационной системе и о виновном лице стали общеизвестными или непосредственно обнаружены органом дознания, следствия (например, в ходе проведения оперативно-розыскных мероприятий по другому делу).

Данные о нарушении целостности и конфиденциальности информации в информационной системе выявлены правоохранительными органами, виновное лицо неизвестно, но заявитель не обратился в правоохранительные органы. Данная проверочная ситуация обусловливается тем, что пострадавший объективно понимает, что выявить виновное лицо сложно. При этом осложняться ситуация может тем, что пострадавший сам, к примеру, сообщил какие-либо конфиденциальные данные, перевел денежные средства непроверенному лицу, что случается достаточно часто.

Значительное место в деятельности по выявлению, раскрытию и расследованию данной категории преступлений занимает производство судебных экспертиз.[[53]](#footnote-53)

Такими экспертизами могут быть судебная программно-компьютерная экспертиза, назначаемая для исследования программного обеспечения, судебная информационно-компьютерная экспертиза, имеющая цель поиск, обнаружение, анализ и оценку информации, подготовленной пользователем или порожденной программами для организации информационных процессов в компьютерной системе, судебная компьютерно-сетевая экспертиза, основывающаяся, прежде всего, на функциональном предназначении компьютерных средств, реализующих какую-либо сетевую информационную технологию. Задачи этой экспертизы включают практически все основные задачи рассмотренных выше видов экспертизы. Это объясняется тем, что её объекты интегрированы из объектов рассмотренных выше видов экспертиз (аппаратные, программные и данные), но лишь с той разницей, что они все функционируют в определенной сетевой технологии.

Таким образом, нестандартность, сложность, многообразие и частое обновление способов совершения преступлений в сфере компьютерной информации и применяемых специальных средств так же накладывают свой отпечаток при расследовании, раскрытии таких преступлений. Методы борьбы с рассматриваемыми преступлениями оказываются недостаточно эффективными, а наличие специальных знаний в области компьютерной техники и программного обеспечения у работников правоохранительных органов является необходимым.

3.2. Повышение эффективности комплекса мероприятий, проводимых в органах внутренних дел, по противодействию и профилактике киберпреступлений

В ведущих странах мира сложилась система концептуальных взглядов на проблемы обеспечения информационной безопасности. Концентрация больших объемов обобщенной и систематизированной информации в организациях (в том числе и в МВД) привела к увеличению возможности утечки секретных и конфиденциальных сведений и к мерам по безопасности информации.

Тем не менее, злоумышленные действия над информацией не уменьшаются, а имеют устойчивую тенденцию роста. Анализ практики показывает, что предпринимаемые действия не всегда носят системный характер, направлены на ликвидацию только отдельных угроз. Одной из причин такого положения дел является незнание или неумелое использование основных принципов и практических подходов к решению проблем информационной безопасности, незнание терминологического аппарата данной предметной области[[54]](#footnote-54).

Раскрытие ключевых терминов предметной области – не самоцель, а формирование на этой основе начальных представлений о целях и задачах защиты информации.

Под информационной безопасностью понимается состояние защищенности информационной среды, при котором исключается возможность ознакомления с информацией (конфиденциальность), изменения или уничтожения (целостность) ее лицами, не имеющими на это права, а также сохраняется возможность ее использования (доступность).

Под защитой информации понимаются любые действия, направленные на обеспечение конфиденциальности, целостности и доступности информации.

Охраняемая зона объекта – ограниченная территория, имеющая обозначенный периметр, на которой принимаются меры по защите информации.

Рубежи защиты – созданные на объекте при помощи организационных и технических мер различные процедуры защиты информации. Главным критерием в выборе средств защиты информации считают ее ценность (реальную или потенциальную).

Ценность информации определяется возможным ущербом от овладения информацией конкурентами, приносимым доходом, а также компенсацией возможных затрат на ее защиту. Для конкурентов же эта ценность должна компенсировать риск, связанный с ее получением (добыванием). Для повышения эффективности защиты информации проводят анализ ее уязвимостей – характерных особенностей и недостатков в защите.

Целью защиты информации является сведение к минимуму потерь, вызванных нарушением целостности данных, их конфиденциальности или недоступности информации для потребителей.

Основными задачами системы информационной безопасности являются[[55]](#footnote-55):

– своевременное выявление и устранение угроз безопасности ресурсам, причин и условий, способствующих финансовому, материальному и моральному ущербу;

– создание механизма и условий оперативного реагирования на угрозы безопасности;

– эффективное пресечение посягательств на ресурсы и угроз персоналу на основе правовых, организационных и инженерно-технических мер и средств обеспечения безопасности;

– создание условий для минимизации и локализации возможного ущерба, ослабления негативного влияния последствий.

Мероприятия по защите информации должны исключать:

– выход электромагнитного и акустического полей, наводок в сетях питания, кабельных линиях, заземлении, радио- и телефонных сетях за пределы контролируемой зоны;

– доступ в помещение, где осуществляется обработка информации, а также визуальные возможности получения информации;

– работу специальных устройств ведения разведки, которые могут находиться в строительных конструкциях помещений и предметах их интерьера, а также внутри самого помещения или непосредственно в средствах обработки и передачи информации;

– перехват информации из каналов передачи данных;

– несанкционированный доступ к информационным ресурсам;

– воздействие излучений, приводящих к разрушению информации.

Приведенная совокупность определений достаточна для формирования общего, пока еще абстрактного взгляда на построение системы информационной безопасности. Для формирования более детального представления необходимо знание основных принципов организации системы информационной безопасности.

Первым и наиболее важным является принцип непрерывного совершенствования системы информационной безопасности. Суть этого принципа заключается в постоянном выявлении слабых мест системы, которые возникают от изменения характера внутренних и внешних угроз.

Вторым является принцип комплексного использования всех доступных средств защиты во всех структурных элементах организации и на всех этапах работы с информацией. Комплексный характер защиты информации проистекает прежде всего из того, что злоумышленники всегда ищут самое слабое звено в системе безопасности.

Важными условиями обеспечения безопасности являются законность, достаточность, соблюдение баланса интересов личности и организации, профессионализм представителей службы безопасности, подготовка пользователей и соблюдение ими всех установленных правил сохранения конфиденциальности, взаимная ответственность персонала и руководства, взаимодействие с государственными правоохранительными органами.

С позиций системного подхода для реализации приведенных принципов процесс да и сама система защиты информации должны отвечать некоторой совокупности требований. Защита информации должна быть[[56]](#footnote-56):

– плановой;

– централизованной;

– активной;

– конкретной и целенаправленной;

– надежной и универсальной;

– нестандартной (по сравнению с другими организациями), разнообразной по используемым средствам;

– открытой для изменения и дополнения; – экономически эффективной: затраты на систему защиты не должны превышать размеры возможного ущерба.

Наряду с основными требованиями, существует ряд устоявшихся рекомендаций, которые будут не бесполезны создателям систем информационной безопасности:

– средства защиты должны быть просты для технического обслуживания и «прозрачны» для пользователей;

– каждый пользователь должен иметь минимальный набор привилегий, необходимых для работы;

– возможность отключения защиты в особых случаях, например, когда механизмы защиты реально мешают выполнению работ;

– независимость системы защиты от субъектов защиты;

– разработчики должны предполагать, что пользователи имеют наихудшие намерения (враждебность окружения), будут совершать серьезные ошибки и искать пути обхода механизмов защиты;

– отсутствие на предприятии излишней информации о существовании механизмов защиты.

Все перечисленные позиции должны лечь в основу формирования системы защиты информации. При обеспечении информационной безопасности существует два аспекта[[57]](#footnote-57):

– формальный, связанный с определением критериев, которым должны соответствовать защищаемые информационные технологии;

– практический, характеризующий порядок определения конкретного комплекса мер безопасности применительно к рассматриваемой информационной технологии.

Критерии, которым должны соответствовать защищаемые информационные технологии, являются объектом стандартизации. В настоящее время разработан проект международного стандарта «Общие критерии оценки безопасности информационных технологий». Содержание подобных документов в основном относится к этапу анализа рисков, на котором определяются угрозы безопасности и уязвимости информационных ресурсов, уточняются требования к режиму информационной безопасности.

Изложенные основные концептуальные положения являются основой механизма выработки детальных предложений по формированию политики и построению системы информационной безопасности.

Необходимо отметить, что использование современных информационных технологий в промышленной, торговой, банковской, научной, культурной, образовательной и других сферах общественной жизни детерминировало динамический рост и качественное обновление компьютерной преступности в России, что создает новые угрозы для развития общества и государства. При этом обеспечение своевременности и эффективности предупредительной деятельности в сфере информационно-телекоммуникационных технологий представляет собой определенную проблему для органов внутренних дел, решение которой во многом зависит от комплексного подхода к разрешению организационных, правовых и методических аспектов специального предупреждения данного вида преступлений.

Развитие информационно-телекоммуникационных технологий позволяет совершать киберпреступления в большинстве случаев безнаказанно, поскольку уголовное законодательство слабо адаптировано к новым видам преступлений в сфере информационных технологий, хотя онлайн-торговля и банковские операции, услуги скоростной передачи данных, современные форматы связи, электронное образование, игровые и развлекательные порталы прочно вошли в жизнь общества и государства.

Повышение роли информационно-телекоммуникационных технологий отразилось и на современных тенденциях киберпреступности:

1. Нарастает, усиливается организованность, расширяются сферы криминальных интересов, усложняются применяемые преступные схемы.

2. Киберпреступления нередко совершаются в совокупности с иными общественно опасными деяниями и имеют факультативный характер. Это обусловлено тем, что, используя компьютерную информацию в качестве средства совершения преступления, преступники «превращают» ее в предмет другого общественно опасного деяния (хищение персональных данных с целью последующего вымогательства). Смещение корыстных интересов преступников в киберпространство произошло вследствие того, что данная криминальная деятельность сверхдоходна и относительно безопасна.

3. Наблюдается переход на транснациональный организованный уровень. Информационно-коммуникационные технологии на современном этапе превратились в удобное для многих преступников средство и орудие совершения любого рода преступлений. При этом постоянно расширяющиеся возможности глобальных сетей обусловили повышенный интерес к ним со стороны организованной преступности, в том числе экстремистских и террористических организаций, так как существующие правила эксплуатации киберпространства позволяют обеспечивать анонимность действий в сети и существенно осложняют идентификацию пользовательского оборудования.

По оценкам специалистов, свыше 80 % киберпреступлений совершаются в той или иной организационных формах, включая формирование единого «теневого рынка» киберпреступности, основанного на постоянной разработке вредоносного программного обеспечения, заражения пользовательских компьютеров, управления бот-сетями, сбора данных личного и финансового характера, продажи похищенных данных. В связи с существованием указанного преступного сегмента подсчитать точное количество преступных кибердеяний, а тем более количество пострадавших от них, невозможно[[58]](#footnote-58).

В реальной действительности предупреждение преступлений представляет собой сложную систему, состоящую из отдельных элементов деятельности разнообразного характера, целью которой служит оказание воздействия на причины и условия, способствующие совершению преступлений, а также на лиц, их совершающих. Деятельность по предупреждению преступлений носит многоуровневый характер, поскольку, помимо масштабных, долговременных, перспективных мер, таких как постановка стратегических задач борьбы с преступностью, нормативного, организационного и ресурсного обеспечения, необходимым является разработка и принятие мер более узкого, конкретного характера, имеющих прикладное значение и рассчитанных на достижение менее крупных, но не менее значимых целей. Предупреждение преступлений, совершаемых с использованием высоких технологий, является одним из приоритетных направлений деятельности органов внутренних дел.

В системе противодействия преступлениям, совершаемым с использованием высоких технологий, целесообразно сосредоточить внимание на разработке нижеперечисленных мер[[59]](#footnote-59).

1. Повышение эффективности научного обеспечения деятельности по противодействию преступности в сфере высоких технологий.

Основным результатом научно-исследовательской работы должен являться адаптированный перенос ее результатов в правоприменительную практику. Координация усилий правоохранительных органов должна осуществляться уже на этапе сбора криминологической информации (начиная с этапа регистрации заявлений и сообщений о преступлениях) и в дальнейшем представлять собой единую информационную систему, позволяющую беспрепятственно обмениваться информацией, в том числе научными разработками и методиками, в процессе предупреждения, раскрытия и расследования высокотехнологичных преступлений.

2. Совершенствование системы правоприменения и разработка новых форм и методов борьбы с преступлениями, совершаемыми с использованием высоких технологий (методическое обеспечение).

Реализация мер по предупреждению высокотехнологичной преступности на данном направлении представляет собой совершенствование подзаконных актов и различного рода инструктивнорегламентирующей документации, которые в силу своей специфики способны оказать оперативное воздействие на ситуацию в случаях, когда законодательное решение проблемы затруднено в силу разных причин. Кроме того, качественное методическое обеспечение способствует эффективному применению законодательных норм в практической деятельности.

К мерам предупреждения преступлений, совершаемых с использованием высоких технологий, также относится разработка новых методик противодействия данному виду преступлений, в том числе в процессе оперативно-розыскной деятельности. Так, представляется необходимым законодательно закрепить полномочия правоохранительных органов на осуществление мониторинга опубликованных в социальных сетях или иных ресурсах материалов противоправного характера, а в некоторых случаях обеспечить проведение соответствующих надзорных, оперативно-розыскных, следственных мероприятий с возможностью получения необходимой информации от провайдеров или Роскомнадзора напрямую без судебного разрешения.

3. Принятие организационно-управленческих мер предупреждения преступлений, совершаемых с использованием высоких технологий. Данное направление характеризуется комплексом мер, направленных на совершенствование деятельности субъектов предупреждения данного вида преступлений. К ним следует отнести[[60]](#footnote-60):

– создание системы подготовки сотрудников правоохранительных органов по специальностям «Защита информации и информационно-телекоммуникационных сетей», «Информационная безопасность» в образовательных учреждениях МВД, ФСБ, МО, ФТС России и др.;

– переход от преимущественно территориального принципа работы правоохранительных органов в сфере предупреждения высокотехнологичной преступности к функциональному;

– совершенствование информационно-аналитического обеспечения деятельности по противодействию преступлениям, совершаемым с использованием высоких технологий. Данная работа связана с решением целого ряда задач, включающих сбор и систематизацию криминологически значимой информации, ее анализ и классификацию, определение на этой основе реальной картины состояния дел и перспективное прогнозирование развития ситуации;

– перевод на новый уровень организации взаимодействия правоохранительных органов со средствами массовой информации. Использование средств массовой информации в системе противодействия высокотехнологичной преступности должно сочетать несколько направлений, таких как отчет перед населением о результатах борьбы с данными преступлениями.

4. Проведение комплекса целенаправленных мероприятий по устранению причин и условий, способствующих совершению компьютерных преступлений в отношении государственных и иных учреждений, предприятий и организаций.

Объектом данной деятельности являются учреждения, предприятия, организации разных форм собственности, пострадавшие или которые могут пострадать в результате преступных посягательств

Отдельно следует остановиться на виктомологическом аспекте противодействия преступлениям, совершаемым с использованием высоких технологий.

Основная работа сотрудников правоохранительных органов должна заключаться прежде всего в доведении до граждан элементарных правил безопасности, таких как недопустимость[[61]](#footnote-61):

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

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

– покупки SIM-карт с рук или оставления своих паспортных данных сомнительным конторам;

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

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

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

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

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

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

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

Итак, виктимологическая профилактика преступлений, совершаемых с использованием высоких технологий, должна быть организована с учетом виктимности различных групп населения; учитывать различные аспекты обеспечения данного вида деятельности; иметь конкретную направленность на осознание необходимости соблюдения мер предосторожности в информационнотелекоммуникационном пространстве; основываться на доступных для населения или работников – неспециалистов рекомендациях по совершенствованию своей защищенности от киберугроз.

Таким образом, изучение международного опыта показывает, что такая тенденция свойственна большинству государств мира. Количество киберпреступлений будет увеличиваться в ближайшем будущем в связи с бурным развитием телекоммуникационных технологий, стремительным увеличением числа электронных устройств и услуг, предоставляемых населению с использованием информационных технологий.

В целях достижения всеобъемлющего, комплексного подхода к проблеме, необходимо объединение усилий государственных органов, общественных объединений, гражданских инициатив, направленных на повышение уровня компьютерной грамотности и цифровой безопасности граждан; развитие и совершенствование систем обеспечения кибербезопасности; мониторинг киберпространства с целью своевременного выявления, предотвращения киберугроз и их нейтрализации; обеспечение защищенности государственных и частных информационных ресурсов от кибератак; создание и совершенствование системы подготовки кадров в сфере кибербезопасности; развитие международного сотрудничества в данной сфере.

ЗАКЛЮЧЕНИЕ

В целях комплексного исследования теоретических и практических проблем противодействия киберпреступности, как фактору обеспечения экономической безопасности государства в работе обоснованы следующие выводы, предложения и рекомендации:

1. Киберпреступность носит ярко выраженный организованный характер, а в большинстве случаев и транснациональный, будучи чрезвычайно прибыльной сферой преступной деятельности. Электронно-вычислительная техника может выступать как средством совершения преступления, так и предметом преступления. Информация становится объектом преступлений: хищения, изменения или уничтожения путем несанкционированного доступа к ней. Киберпреступность содержит не только техническую и правовую, но и социальную проблему, эффективное решение которой требует, прежде всего, системного подхода к разработке основ обеспечения безопасности жизненно важных интересов гражданина, общества и государства в киберпространстве.

2. Современная киберпреступность является не только результатом стремительного развития информационных технологий, но и важной и чрезвычайно прибыльной сферой преступной деятельности. Практически ни одно государство не стоит в стороне от данной проблемы. Направляя свои усилия на снижение рисков ее проявления на собственной территории, государства действуют в активном сотрудничестве, взаимопомощи и координации действий направленных на противодействие киберпреступности.

3. На текущий момент киберпреступление является одной из самых быстро растущих категорий преступлений в России. Развитие киберпреступности идет в ногу с развитием информационно-технических средств, а мотивы киберпреступников также видоизменяются с развитием таких преступлений. Кибератаки стали массовым явлением, а их направления задевают все сферы общества.

Стоит констатировать, что предпосылки зарождения и развития киберпреступности формировались в России в течение последних нескольких лет. Во-первых, это цифровизация различных сторон жизнедеятельности россиян: например, высокий интерес к банковским картам и счетам, безналичным способам оплаты, онлайн-досуг и активное использование соцсетей. Во-вторых, сохраняющийся низкий уровень цифровых компетенций граждан страны. В-третьих, низкая квалификация правоохранительных органов, несовершенство антифрод-инфраструктуры, неспособность оперативно пресекать киберпреступную деятельность и эффективно расследовать инциденты в цифровой среде.

4. Несколько лет назад был не замечен или проигнорирован тренд на зарождение новой масштабной социальной проблемы в России – киберпреступности. Было упущено время на работу с населением, подготовку инфраструктуры, соответствующих подразделений, налаживание международного сотрудничества и выстраивание законодательной базы. Сейчас можно наблюдать поспешные действия в попытке исправить ситуацию, которая становится все более критической: создание в МВД РФ и Следственном комитете подразделений по борьбе с киберпреступностью, работа по информированию граждан о новых видах мошеннических схем, запуск специальной платформы для борьбы с мошенничеством, международное сотрудничество на высочайшем уровне, технологии по определению телефонных мошенников со стороны банковского сектора. Тем не менее сторона противодействия преступной деятельности в данном противостоянии занимает на текущий момент отстающую позицию: количество киберпреступлений продолжает расти.

5. Нестандартность, сложность, многообразие и частое обновление способов совершения преступлений в сфере компьютерной информации и применяемых специальных средств так же накладывают свой отпечаток при расследовании, раскрытии таких преступлений. Методы борьбы с рассматриваемыми преступлениями оказываются недостаточно эффективными, а наличие специальных знаний в области компьютерной техники и программного обеспечения у работников правоохранительных органов является необходимым.

6. Изучение международного опыта показывает, что такая тенденция свойственна большинству государств мира. Количество киберпреступлений будет увеличиваться в ближайшем будущем в связи с бурным развитием телекоммуникационных технологий, стремительным увеличением числа электронных устройств и услуг, предоставляемых населению с использованием информационных технологий.

В целях достижения всеобъемлющего, комплексного подхода к проблеме, необходимо объединение усилий государственных органов, общественных объединений, гражданских инициатив, направленных на повышение уровня компьютерной грамотности и цифровой безопасности граждан; развитие и совершенствование систем обеспечения кибербезопасности; мониторинг киберпространства с целью своевременного выявления, предотвращения киберугроз и их нейтрализации; обеспечение защищенности государственных и частных информационных ресурсов от кибератак; создание и совершенствование системы подготовки кадров в сфере кибербезопасности; развитие международного сотрудничества в данной сфере.

список использованных источников

Нормативные правовые акты

1. Конституция Российской Федерации: принята всенародным голосованием 12.12.1993 г. (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ, от 04.07. 2020 г. № 1-ФКЗ) // СЗ РФ. – 2014. – № 31.
2. Конвенция о защите физических лиц при автоматизированной обработке персональных данных (Заключена в г. Страсбурге 28.01.1981) // Собр. законодательства РФ. – 2014. – № 5. – ст. 419.
3. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ (ред. 28.12.2016): офиц. текст // Собрание законодательства. – 1994. - №32. – Ст. 3301.
4. Уголовный кодекс Российской Федерации от 13 июня 1996 года № 63-ФЗ (с изм. от 29 июля 2017 г. № 250-ФЗ) // Собрание законодательства РФ.- 1996. - № 25. - ст. 2954.
5. [Уголовно-процессуальный кодекс РФ](http://ru.wikipedia.org/wiki/%D0%A3%D0%B3%D0%BE%D0%BB%D0%BE%D0%B2%D0%BD%D0%BE-%D0%BF%D1%80%D0%BE%D1%86%D0%B5%D1%81%D1%81%D1%83%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D0%B9_%D0%BA%D0%BE%D0%B4%D0%B5%D0%BA%D1%81_%D0%A0%D0%A4) от 18.12.2001 [№ 174-ФЗ](http://ru.wikisource.org/wiki/%D0%A3%D0%B3%D0%BE%D0%BB%D0%BE%D0%B2%D0%BD%D0%BE-%D0%BF%D1%80%D0%BE%D1%86%D0%B5%D1%81%D1%81%D1%83%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D0%B9_%D0%BA%D0%BE%D0%B4%D0%B5%D0%BA%D1%81_%D0%A0%D0%A4) (с изм. от 21 декабря 2013 г. № 376-ФЗ) // Собрание законодательства РФ.- 2001.- № 52 (ч. I), ст. 4921.
6. Федеральный закон от 27.06.2011 № 161-ФЗ «О национальной платежной системе» // СЗ РФ. – 2011. – № 27. – ст. 3872.
7. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СЗ РФ. – 2006. – № 31. – ст. 3448.
8. Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СЗ РФ. – 2016. – № 50. – ст. 7074.

Научная и учебная литература

1. Аносов А.В. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: учеб. пособие / А. В. Аносов. – М.: Академия управления МВД России, 2019. – 208 с.
2. Васильчикова Н.В. Криминология: учеб.пособие / Н.В. Васильчикова. – М.: Юрайт-Издат, 2016. – 144 с.
3. Долгова А.И. Криминология: учебный курс / А.И. Долгова. – М.: Норма, 2018. – 368 с.
4. Мтяйло Н.Э. Киберпреступления как проявление современной организационной преступности // Науки Европы. – 2018. – № 26. – С.46-52.
5. Россинская Е.Р. Криминалистика: учебник / Е.Р. Россинская. – М.: Норма, 2017. – 464 с.
6. Русскевич Е.А. Уголовное право и «цифровая преступность»: проблемы и решения: монография / Е.А. Русскевич. – М.: ИНФРА-М, 2019. – 227с.
7. Тюнис И.О. Криминалистика: учебное пособие / И.О. Тюнис. – М.: МФПУ Синергия, 2016. – 232 с.
8. Яблоков Н.П. Криминалистическая методика расследования: современное состояние и проблемы: монография / Н.П. Яблоков. – М.: ИНФРА-М, 2016. – 192 с.

Научные статьи

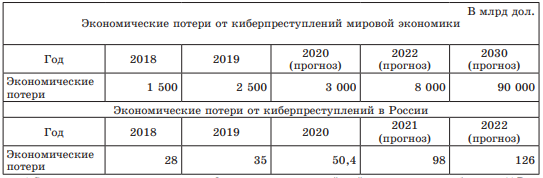
1. Артамонов В.А. Кибербезопасность в условиях цифровой трансформации социума / В.А. Артамонов // Большая Евразия: развитие, безопасность, сотрудничество. – 2022. – № 1. – С.777-784.
2. Ахриева М.М. Киберпреступность в условиях современной экономики / М.М. Ахриева // Международный журнал гуманитарных и естественных наук. – 2021. – № 8-2 (59). – С.80-82.
3. Дерюгин Р.А. Киберпреступность в России: современное состояние и актуальные проблемы / Р.А. Дерюгин // Вестник Уральского юридического института МВД России. – 2018. – № 2. – С.46-49.
4. Диденко К.В. Некоторые проблемы выявления и предупреждения киберпреступлений / К.В. Диденко // Вестник БЮИ МВД России. – 2020. – № 3. – С.20-24.
5. Маслиенко М.А. Киберпреступность на современном этапе / М.А. Маслиенко // Проблемы правоохранительной деятельности. – 2021. – № 2. – С.28-32.
6. Осипенко А.Л. Об участии органов внутренних дел в системе обеспечения кибербезопасности Российской Федерации / А.Л. Осипенко // Общество и право. – 2018. – № 3 (65). – С.35-43.
7. Русакова О.И. Влияние киберпреступлений на банковскую систему России / О.И.Русакова // [Baikal Research Journal](https://cyberleninka.ru/journal/n/baikal-research-journal). – 2021. – № 1. – С.1-12.
8. Самурханов М.С. Понятие и особенности киберпреступности / М.С. Самурханов // Международный журнал гуманитарных и естественных наук. – 2020. – № 4-3 (43). – С.219-221.
9. Сафонова М.Ф. Кибербезопасность: проблемы и решения / М.Ф. Сафонова // Естественно-гуманитарные исследования. – 2019. – № 24(2). – С.63-68.
10. Пелевина А.В. Общая характеристика преступлений в сфере компьютерной информации // Проблемы в российском законодательстве. – 2015. – № 1. – С.1-3.
11. Потапов С.А. Совершенствование расследования и раскрытия преступлений в сфере компьютерной информации // Социально-экономические явления и процессы. – 2016. – № 10. – С.90-95.
12. Рахимова У.Х. Предмет киберпреступления и предел доказательства // [Правовой отчет TSUL](https://cyberleninka.ru/journal/n/tsul-legal-report). – 2020. – № 1. – С.100-110.
13. Тиханычева Е.О. «Цифровая экономика» как эволюция с революционными последствиями / Е.О. Тиханычева // [The Scientific Heritage](https://cyberleninka.ru/journal/n/the-scientific-heritage). – 2022. – № 82. – С.58-64.
14. Шевко Н.Р. Кибербезопасность: проблемы и пути решения / Н.Р. Шевко // Вестник экономической безопасности. – 2020. – № 5. – С.185-189.
15. Швыряев П.С. Киберпреступность в России: новый вызов для общества и государства / П.С. Швыряев // Государственное управление. – 2021. – № 89. – С.184-196.

Интернет – источники

1. Кибербезопасность 2019—2020: тенденции и прогнозы // Режим доступа: URL: [https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/ cybersecurity-2019-2020-rus.pdf](https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/%20cybersecurity-2019-2020-rus.pdf)
2. Киберпреступлений становится все больше, однако их раскрываемость уменьшается [Электронный ресурс] // Режим доступа: URL: https://www.advgazeta.ru
3. О преступлениях, совершаемых с использованием современных информационно-коммуникационных технологий [Электронный ресурс] // Генеральная прокуратура Российской Федерации [сайт]. URL: [https://genproc.gov.ru](https://genproc.gov.ru/smi/news/news-1431104/)
4. Приговоры судов по ст. 272 УК РФ Неправомерный доступ к компьютерной информации [Электронный ресурс] // Режим доступа: URL: http://sud-praktika.rul
5. Состояние преступности. Статистика Министерство Внутренних Дел РФ. URL: <http://www.mvd.ru>
6. Статистические данные [Электронный ресурс] // Федеральная служба исполнения наказаний Российской Федерации [сайт]. URL: http://www.fsin.su
7. Экономические последствия расширения масштабов киберпреступности в России и мире Электронный ресурс] // Федеральная служба исполнения наказаний Российской Федерации [сайт]. URL: https://wiselawyer.ru/poleznoe/101697-ekonomicheskie-posledstviya-rasshireniya-masshtabov-kiberprestupnosti-rossii-mire

Приложение 1

Экономические потери от киберпреступлений



|  |  |
| --- | --- |
| [**КНИЖНЫЙ МАГАЗИН**](http://учебники.информ2000.рф/chitai.shtml) |  |

|  |  |
| --- | --- |
| [**ТОВАРЫ для ХУДОЖНИКОВ и ДИЗАЙНЕРОВ**](http://учебники.информ2000.рф/kar.shtml) |  |

|  |  |
| --- | --- |
| [**АУДИОЛЕКЦИИ**](http://учебники.информ2000.рф/lectr.shtml) |  |

|  |  |
| --- | --- |
| [**IT-специалисты: ПОВЫШЕНИЕ КВАЛИФИКАЦИИ**](http://учебники.информ2000.рф/otu.shtml) |  |

|  |  |
| --- | --- |
| [**ФИТНЕС на ДОМУ**](http://учебники.информ2000.рф/fit1.shtml) |  |

1. См. Артамонов В.А. Кибербезопасность в условиях цифровой трансформации социума // Большая Евразия: развитие, безопасность, сотрудничество. – 2022. – № 1. – С.777. [↑](#footnote-ref-1)
2. См. Рахимова У.Х. Предмет киберпреступления и предел доказательства // [Правовой отчет TSUL](https://cyberleninka.ru/journal/n/tsul-legal-report). – 2020. – № 1. – С.100. [↑](#footnote-ref-2)
3. См. Мтяйло Н.Э. Киберпреступления как проявление современной организационной преступности // Науки Европы. – 2018. – № 26. – С.47. [↑](#footnote-ref-3)
4. См. Зубова М. А. Компьютерная информация как объект уголовно-правовой охраны: Автореф. дисс. …  канд. юрид. наук. – Казань, 2008. – С.10. [↑](#footnote-ref-4)
5. См. Суслопаров А.В.  Информационные преступления: Автореф. дисс. …  канд. юрид. наук. – Красноярск, 2008. – С. 9. [↑](#footnote-ref-5)
6. См. Сверчков В.В. Уголовное право. Общая и Особенная части: учеб. пособие. – М.: Высшее образование, 2008. – С. 503. [↑](#footnote-ref-6)
7. См. Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: дис.канд. юрид.наук. Владивосток. - 2005. С.36. [↑](#footnote-ref-7)
8. См. Самурханов М.С. Понятие и особенности киберпреступности // Международный журнал гуманитарных и естественных наук. – 2020. – № 4-3 (43). – С.220. [↑](#footnote-ref-8)
9. См. Гаджиев М.С. Криминологический анализ преступности в сфере компьютерной информации): автореф. дис.... канд. юрид. наук. Махачкала, 2004. С. 9. [↑](#footnote-ref-9)
10. См. Ахриева М.М. Киберпреступность в условиях современной экономики // Международный журнал гуманитарных и естественных наук. – 2021. – № 8-2 (59). – С.80. [↑](#footnote-ref-10)
11. См. Сафонов О.М. Уголовно-правовая оценка использования компьютерных технологий при совершении преступлений: состояние законодательства и правоприменительной практики, перспективы совершенствования: дис. ... канд. юрид. наук. – М.- 2015. – С.83. [↑](#footnote-ref-11)
12. См. Гузеева О.С. Квалификация преступлений в сфере компьютерной информации. – М.- 2016. – С.29. [↑](#footnote-ref-12)
13. См. Ефремова М.А. Уголовно-правовая охрана информационной безопасности: автореф. дис.... д-ра юрид. наук. – М.- 2018. – С.47. [↑](#footnote-ref-13)
14. См. Мтяйло Н.Э. Киберпреступления как проявление современной организационной преступности // Науки Европы. – 2018. – № 26. – С.47. [↑](#footnote-ref-14)
15. См. Мтяйло Н.Э. Киберпреступления как проявление современной организационной преступности // Науки Европы. – 2018. – № 26. – С.47. [↑](#footnote-ref-15)
16. См. Рахимова У.Х. Предмет киберпреступления и предел доказательства // [Правовой отчет TSUL](https://cyberleninka.ru/journal/n/tsul-legal-report). – 2020. – № 1. – С.101. [↑](#footnote-ref-16)
17. См. Русакова О.И. Влияние киберпреступлений на банковскую систему России // [Baikal Research Journal](https://cyberleninka.ru/journal/n/baikal-research-journal). – 2021. – № 1. – С.5. [↑](#footnote-ref-17)
18. См. Ахриева М.М. Киберпреступность в условиях современной экономики // Международный журнал гуманитарных и естественных наук. – 2021. – № 8-2 (59). – С.80. [↑](#footnote-ref-18)
19. См. Экономические последствия расширения масштабов киберпреступности в России и мире Электронный ресурс] // Федеральная служба исполнения наказаний Российской Федерации [сайт]. URL: https://wiselawyer.ru/poleznoe/101697-ekonomicheskie-posledstviya-rasshireniya-masshtabov-kiberprestupnosti-rossii-mire [↑](#footnote-ref-19)
20. См. Рахимова У.Х. Предмет киберпреступления и предел доказательства // [Правовой отчет TSUL](https://cyberleninka.ru/journal/n/tsul-legal-report). – 2020. – № 1. – С.102. [↑](#footnote-ref-20)
21. См. Рахимова У.Х. Предмет киберпреступления и предел доказательства // [Правовой отчет TSUL](https://cyberleninka.ru/journal/n/tsul-legal-report). – 2020. – № 1. – С.103. [↑](#footnote-ref-21)
22. См. Диденко К.В. Некоторые проблемы выявления и предупреждения киберпреступлений // Вестник БЮИ МВД России. – 2020. – № 3. – С.22. [↑](#footnote-ref-22)
23. См. Министерство внутренних дел [Электронный ресурс]. – Режим доступа: <https://xn--b1aew.xn--p1ai/mvd/structure1/Upravlenija/Upravlenie_K_MVD_Rossii>. [↑](#footnote-ref-23)
24. См. Топорков А.А. Криминалистика: учебник. – М.: КОНТРАКТ, ИНФРА-М, 2017. – С. 365. [↑](#footnote-ref-24)
25. См. Шевко Н.Р. Кибербезопасность: проблемы и пути решения // Вестник экономической безопасности. – 2020. – № 5. – С.186. [↑](#footnote-ref-25)
26. См. Русакова О.И. Влияние киберпреступлений на банковскую систему России // [Baikal Research Journal](https://cyberleninka.ru/journal/n/baikal-research-journal). – 2021. – № 1. – С.5. [↑](#footnote-ref-26)
27. См. Русакова О.И. Влияние киберпреступлений на банковскую систему России // [Baikal Research Journal](https://cyberleninka.ru/journal/n/baikal-research-journal). – 2021. – № 1. – С.8. [↑](#footnote-ref-27)
28. См. Шевко Н.Р. Кибербезопасность: проблемы и пути решения // Вестник экономической безопасности. – 2020. – № 5. – С.186. [↑](#footnote-ref-28)
29. См. Шевко Н.Р. Кибербезопасность: проблемы и пути решения // Вестник экономической безопасности. – 2020. – № 5. – С.187. [↑](#footnote-ref-29)
30. См. Ахриева М.М. Киберпреступность в условиях современной экономики // Международный журнал гуманитарных и естественных наук. – 2021. – № 8-2 (59). – С.81. [↑](#footnote-ref-30)
31. См. Шевко Н.Р. Кибербезопасность: проблемы и пути решения // Вестник экономической безопасности. – 2020. – № 5. – С.188. [↑](#footnote-ref-31)
32. См. Швыряев П.С. Киберпреступность в России: новый вызов для общества и государства // Государственное управление. – 2021. – № 89. – С.188. [↑](#footnote-ref-32)
33. См. Ахриева М.М. Киберпреступность в условиях современной экономики // Международный журнал гуманитарных и естественных наук. – 2021. – № 8-2 (59). – С.81. [↑](#footnote-ref-33)
34. См. Швыряев П.С. Киберпреступность в России: новый вызов для общества и государства // Государственное управление. – 2021. – № 89. – С.189. [↑](#footnote-ref-34)
35. См. Ахриева М.М. Киберпреступность в условиях современной экономики // Международный журнал гуманитарных и естественных наук. – 2021. – № 8-2 (59). – С.81. [↑](#footnote-ref-35)
36. См. Киберпреступлений становится все больше, однако их раскрываемость уменьшается [Электронный ресурс] // Режим доступа: URL: https://www.advgazeta.ru [↑](#footnote-ref-36)
37. См. Швыряев П.С. Киберпреступность в России: новый вызов для общества и государства // Государственное управление. – 2021. – № 89. – С.191. [↑](#footnote-ref-37)
38. См. Киберпреступлений становится все больше, однако их раскрываемость уменьшается [Электронный ресурс] // Режим доступа: URL: https://www.advgazeta.ru [↑](#footnote-ref-38)
39. См. Киберпреступлений становится все больше, однако их раскрываемость уменьшается [Электронный ресурс] // Режим доступа: URL: https://www.advgazeta.ru [↑](#footnote-ref-39)
40. См. Шевко Н.Р. Кибербезопасность: проблемы и пути решения // Вестник экономической безопасности. – 2020. – № 5. – С.188. [↑](#footnote-ref-40)
41. Швыряев П.С. Киберпреступность в России: новый вызов для общества и государства // Государственное управление. – 2021. – № 89. – С.191. [↑](#footnote-ref-41)
42. См. Герасимова Л.Я. Криминалистика: учебник. – М.: Высш. шк., 2019. – С. 346. [↑](#footnote-ref-42)
43. См. Степанов-Егиянц В.Г. Современная уголовная политика в сфере борьбы с компьютерными преступлениями // Российский следователь. – 2012. – № 24. – С. 45. [↑](#footnote-ref-43)
44. См. Ищенко Е.П. Криминалистика: учебник. – М.: КОНТРАКТ, ИНФРА-М, 2010. – С. 564. [↑](#footnote-ref-44)
45. См. Гаврилин Ю.В. Особенности следообразования при совершении мошенничеств в сфере компьютерной информации // Российский следователь. – 2013. – № 23. – С. 5. [↑](#footnote-ref-45)
46. См. Гаврилин Ю.В. Особенности следообразования при совершении мошенничеств в сфере компьютерной информации // Российский следователь. – 2013. – № 23. – С. 6. [↑](#footnote-ref-46)
47. См. Осипенко А.Л. Особенности расследования сетевых компьютерных преступлений // Российский юридический журнал. – 2010. – № 2. – С. 125. [↑](#footnote-ref-47)
48. См. Ищенко Е.П. Криминалистика: учебник. – М.: КОНТРАКТ, ИНФРА-М, 2010. – С. 564. [↑](#footnote-ref-48)
49. См. Осипенко А.Л. Особенности расследования сетевых компьютерных преступлений // Российский юридический журнал. – 2010. – № 2. – С. 124. [↑](#footnote-ref-49)
50. См. Куровин Н.К. Криминалистика: учебное пособие. – Новосибирск: Издательство НГТУ, 2015. – С. 101. [↑](#footnote-ref-50)
51. См. Министерство внутренних дел [Электронный ресурс]. – Режим доступа: <https://xn--b1aew.xn--p1ai/mvd/structure1/Upravlenija/Upravlenie_K_MVD_Rossii>. Дата обращения: 10.11.2019. [↑](#footnote-ref-51)
52. См. Потапов С.А. Совершенствование расследования и раскрытия преступлений в сфере компьютерной информации // Cоциально-экономические явления и процессы. Т.11. Тамбов, 2016. № 10. С. 92. [↑](#footnote-ref-52)
53. Егорышева Е.А. Некоторые вопросы использования специальных знаний при расследовании неправомерного доступа к компьютерной информации. Эксперт-криминалист, 2011. № 3. С. 14. [↑](#footnote-ref-53)
54. См. Аносов А.В. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: учеб. пособие. – М.: Академия управления МВД России, 2019. – С.36. [↑](#footnote-ref-54)
55. См. Аносов А.В. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: учеб. пособие. – М.: Академия управления МВД России, 2019. – С.37. [↑](#footnote-ref-55)
56. См. Аносов А.В. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: учеб. пособие. – М.: Академия управления МВД России, 2019. – С.38. [↑](#footnote-ref-56)
57. См. Аносов А.В. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: учеб. пособие. – М.: Академия управления МВД России, 2019. – С.39. [↑](#footnote-ref-57)
58. См. Аносов А.В. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: учеб. пособие. – М.: Академия управления МВД России, 2019. – С.59. [↑](#footnote-ref-58)
59. См. Аносов А.В. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: учеб. пособие. – М.: Академия управления МВД России, 2019. – С.64. [↑](#footnote-ref-59)
60. См. Аносов А.В. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: учеб. пособие. – М.: Академия управления МВД России, 2019. – С.66. [↑](#footnote-ref-60)
61. См. Аносов А.В. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: учеб. пособие. – М.: Академия управления МВД России, 2019. – С.71. [↑](#footnote-ref-61)