**БЕЛГОРОДСКИЙ ЮРИДИЧЕСКИЙ ИНСТИТУТ МВД РОССИИ
ИМЕНИ И.Д. ПУТИЛИНА**

А.А. Дрога, С.Е. Савотченко, В.Л. Акапьев

ИСПОЛЬЗОВАНИЕ ОСОБЕННОСТЕЙ СИСТЕМНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПНОСТИ В СФЕРЕ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Учебное пособие

**Белгород
Белгородский юридический институт МВД России
имени И.Д. Путилина
2023**

УДК 004.056
ББК 67.401.133
Д 75

Печатается по решению
редакционно-издательского совета
Бел ЮИ МВД России
имени И.Д. Путилина

Дрога А.А.

Использование особенностей системного программного обеспечения
Д 75 для противодействия преступности в сфере информационно-телекоммуникационных технологий: учебное пособие / А.А. Дрога, С.Е. Савотченко, В.Л. Акапьев.– Белгород: Бел ЮИ МВД России имени И.Д. Путилина, 2023. – 76 с.

ISBN 978-5-91776-484-9

Рецензенты:

Старостенко И.Н., кандидат физико-математических наук, доцент (Краснодарский университет МВД России);

Дубинина Н.М., кандидат юридических наук, доцент (Московский университет МВД России имени В.Ф. Кикотя).

В учебном пособии рассмотрены основные аспекты возможности использования системного программного обеспечения для противодействия преступлениям в сфере информационных технологий. Дана характеристика преступлений в сфере информационных технологий. Рассмотрены правовые аспекты и мероприятия по противодействию преступлениям в сфере информационных технологий. Проведен анализ состава и объема рынка системного программного обеспечения в противодействии преступлениям в сфере информационных технологий.

Предназначено для курсантов и слушателей, профессорско-преподавательского состава, слушателей факультета заочного обучения образовательных организаций системы МВД России, лиц рядового состава и младшего начальствующего состава, впервые принятых на службу в органы внутренних дел Российской Федерации по должности служащего «Полицейский», лиц среднего и старшего начальствующего состава, впервые принятых на службу в органы внутренних дел Российской Федерации по должности служащего «Полицейский», имеющих высшее или среднее профессиональное (неюридическое) образование.

УДК 004.056
ББК 67.401.133

ISBN 978-5-91776-484-9

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Деятельность в правоохранительных органах Российской Федерации на современном этапе развития информационного общества в связи с активным ростом компьютерных преступлений требует использования новейших информационных технологий [7, с. 21]. Особую актуальность приобретают информационные технологии, основанные на использовании специального системного программного обеспечения [6, с. 14], в контексте импортозамещения [18, с. 114], направленного на повышение информационной безопасности и защиты информации [7, с. 11; 8, с. 23; 9, с. 18; 10, с. 12]. Поскольку уровень информационной компетентности сотрудника и его профессиональная подготовка напрямую определяют оперативность его служебной деятельности и качество достигаемых результатов [5, с. 35; 16, с. 11], то возникает необходимость повышения эффективности практико-ориентированного обучения в направлении использования специального системного программного обеспечения [28, с. 5; 73; 85].

Количественный и качественный состав программного обеспечения, используемого в правоохранительной деятельности, предъявляют повышенные требования к сотрудникам ОВД, обязанным применять современные информационные технологии в своей повседневной деятельности [23, с. 147; 26, с. 132]. В связи с необходимостью обучения навыкам использования постоянно совершенствующихся информационных технологий и обновляющегося системного программного обеспечения, важнейшую роль в подготовке квалифицированных специалистов играет система профессионального образования [25, с. 168; 27, с. 21].

В рамках компетентностного подхода современная система подготовки профессиональных кадров для ОВД позволяет сформировать уровень информационно-коммуникационной компетентности [78; 79; 88], необходимый для эффективного и оперативного решения специальных задач с использованием информационных технологий [19, с. 175]. Совершенствование навыков использования системного программного обеспечения становится особенно актуальным в контексте развивающегося в последнее время импортозамещения.

Возникает необходимость проведения анализа системного программного обеспечения для противодействия киберпреступлениям, его актуальность, уровень защиты, а также его место и роль в обеспечении информационной безопасности и борьбы правоохранительных органов с ростом числа преступлений в сфере информационных технологий [3; 17, с. 35].

В свою очередь, это обуславливает необходимость актуализации применения системного программного обеспечения и информационных технологий для противодействия компьютерным преступлениям в условиях формирования информационно-технологической компетентности сотрудников ОВД.

Материалы пособия могут быть использованы в образовательном процессе образовательных организаций системы МВД России по учебным дисциплинам «Информатика и информационные технологии в профессиональной деятельности» по направлению подготовки 40.05.01 «Правовое обеспечение национальной безопасности», «Информационно-коммуникационные технологии в профессиональной служебной деятельности» по направлению подготовки 40.03.02 «Обеспечение законности и правопорядка», в том числе и с использованием элементов технологий дистанционного обучения.

ГЛАВА 1.
ОБЩАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙВ СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

1.1. Подходы к понятию преступлений в сфере информационных технологий

Современный уровень развития информационных технологий (ИТ или IT-технологии) и цифровизация российского пространства привели к модернизации преступности. В настоящее время преступники нацелены на поиск наиболее благоприятных условий и среды совершения преступлений. Информационно-телекоммуникационные технологии (ИКТ) стали площадкой для преступности. Стоит отметить, что с каждым годом преступность с использованием информационно-телекоммуникационных технологий приобретает все более «изощренные» формы. Происходит совершенствование способов совершения преступлений, появляются новые способы распространения вредоносных программ, способных нанести существенный ущерб нормальному функционированию и использованию информационно-телекоммуникационных технологий [31, с. 11]. Большинство противоправных деяний, совершаемых с использованием информационно-телекоммуникационных технологий уже являются преступными и наказуемыми с точки зрения Уголовного кодекса Российской Федерации (далее – УК РФ).

Преступления, совершаемые с использованием информационно-телекоммуникационных технологий, в условиях современной цифровой действительности стали занимать значительную долю среди всех совершенных преступлений. Актуальное значение приобретает проблема борьбы с преступлениями, совершенными с использованием информационно-телекоммуникационных технологий [11, с. 26].

Стоит отметить, что данную группу преступлений нельзя объединить по объекту уголовно-правовой охраны, поскольку использование информационно-телекоммуникационных технологий при совершении преступления отражает лишь способ совершения преступления. Потому будет дана уголовно-правовая характеристика тех преступлений, при совершении которых преступник прибегает к использованию информационно-телекоммуникационных технологий.

Кроме того, в действующем УК РФ не встретится понятие преступлений, совершенных с использованием информационно-телекоммуникационных технологий, потому представляется необходимым обратиться к доктринальному толкованию данного понятия [34, с. 14].

Прежде всего, предлагается обратить внимание на тот момент, что преступления, совершенные с использованием информационно-телекоммуникационных технологий, в юридической литературе именуются по-разному. Например, можно встретить такие названия, как «***компьютерные преступления***», «***информационные преступления***», «***киберпреступления***», «***интернет-***

преступления», «***преступления в IT-сфере***», «***IT-преступления***», «***преступления в сфере компьютерной информации***» и многие другие.

Т.Г. Смирнова писала: «Под ***преступлениями в сфере компьютерной информации*** понимаются запрещенные уголовным законом общественно опасные виновные деяния, которые причиняют либо создают угрозу причинения вреда жизни, здоровью личности, правам и свободам человека и гражданина, государственной и общественной безопасности» [17, с. 42]. Однако в условиях современности данное определение является совершенно несостоятельным.

Это объясняется тем, что в настоящее время использование информационно-телекоммуникационных технологий является способом совершения различных по своим уголовно-правовым характеристикам преступлений. К тому же в настоящее время список средств, используемых для совершения преступлений в качестве информационно-телекоммуникационных технологий, не ограничивается одним компьютером.

А.С. Унукович выказывает наиболее современный взгляд на понятие преступлений, совершаемых с использованием информационно-телекоммуникационных технологий [53, с. 279]. Автор обращает внимание, что использование информационно-телекоммуникационных технологий происходит в новой среде – в виртуальном пространстве. Основу виртуального пространства (за счет чего и происходит моделирование виртуальной среды) составляют информационно-телекоммуникационные технологии. В виртуальной среде смоделированы те элементы, которые имеют место в реальной действительности – это данные о лицах, предметах, фактах, определенных обстоятельствах.

Описывая технологическую сторону процесса воспроизведения сведений, данных из действительности в виртуальной среде, автор указывает, что они приобретают форму электрических сигналов, находящихся в непрерывном движении в информационно-телекоммуникационных сетях. Виртуальные данные хранятся в устройствах памяти на физических носителях или в виртуальной форме.

Т.П. Кесарев также предлагает отграничивать информационные преступления и компьютерные преступления [11, с. 26]. По мнению автора, компьютерные преступления являются лишь частью преступлений, совершенных с использованием информационно-телекоммуникационных технологий. Автор также утверждает, что преступления, совершаемые с использованием информационно-телекоммуникационных систем и технологий, являются составной частью компьютерной преступности, форма которой так актуальна для нашего времени. Т.П. Кесарев ограничивается тем, что под преступлениями в информационной телекоммуникационной сети Интернет следует понимать запрещенные уголовным законом деяния, связанные с использованием сети Интернет и компьютерной техники.

Под ***преступлениями, совершенными с использованием информационно-телекоммуникационных технологий***, следует понимать виновно совершенные общественно опасные деяния в информационно-цифровой сфере, а также с использованием информационно-телекоммуникационных технологий,

причиняющие вред охраняемым уголовным законом правам и интересам граждан, организаций и государства.

Некоторые авторы справедливо отмечают, что стремительное развитие преступности в информационно-коммуникационной среде и с использованием информационно-коммуникационных технологий при совершении преступлений требует совершенствования национальной системы права [32, с. 104; 54, с. 118]. Например, по мнению Е.Д. Василькова, необходима разработка профильного нормативного правового акта, закрепляющего основополагающие понятия [31, с. 12]. Автор отмечает, что современный комплекс борьбы с преступностью с использованием информационно-телекоммуникационных технологий требует совершенствования не только частной криминалистической методики расследования соответствующей группы преступлений, но и разработки соответствующего правового фундамента, закрепляющего основополагающие понятия.

Это утверждение справедливо относится к разработке на законодательном уровне таких ключевых понятий, как «компьютерная преступность», «киберпреступность» и др.

1.2. Систематизация и классификация преступлений в сфере информационных технологий

В современном мире практически каждый человек использует компьютерную технику и сеть Интернет. Информационные технологии влияют как на жизнь конкретных людей, их образование и рабочую сферу, так и на взаимодействие гражданского общества и государства, на развитие мировой экономики. Кроме того, события последних лет все сильнее перемещают обычное функционирование жизни в информационное пространство. Так и преступления, совершаемые с использованием компьютерных технологий, стали довольно широким понятием, включающим большую часть предусмотренных УК РФ составов преступлений [4]. Министерство внутренних дел, в свою очередь, относит к подобным преступлениям мошенничество и кражи, совершаемые с использованием ИТ-технологий. Однако проблема уголовно-правовых рисков с использованием информационных технологий является в значительной степени более масштабной.

Преступления в сфере компьютерной информации – это те деяния, которые совершаются в сфере информационных процессов и посягают на информационную безопасность. Их предметом являются информация и компьютерные средства, в том числе и программное обеспечение [71].

Благодаря распространению таких преступлений развивается ***киберпреступность***. Это такая преступность, которая распространяется в виртуальном пространстве, то есть в информационной среде, моделируемой с помощью компьютера, в которой располагается большое количество важных сведений и о лицах, и о предметах, и о событиях окружающего мира, находящихся в процес-

се движения по локальным и глобальным компьютерным сетям. Так, к киберпреступлениям может быть отнесено любое преступление, совершенное в электронной среде [77].

Обозначим отличительные особенности киберпреступлений. Во-первых, это латентность IT-преступлений. В сфере компьютерных правонарушений распространены незарегистрированные деяния, которые называют скрытой частью преступности. Не все их можно легко обнаружить, а тем более раскрыть по причине большой развернутости способов и методов, а также возможности не оставить биологического следа (кожа, ноготь и другие биоматериалы), по которому обнаруживается подозреваемый [36, с. 75]. Однако следы все-таки остаются. Их называют промежуточными между материальными и идеальными, или «виртуальными». Такие следы сохраняются в памяти технических устройств, в электромагнитном поле, на машинных носителях компьютерной информации, и они не могут быть изъяты. Однако есть возможность копирования таких данных и при наличии такой потребности необходимо действовать оперативно, так как их хранение в соответствующих местах довольно кратковременно. Во-вторых, данный вид преступности характеризуется трансграничностью, то есть такой организованной системой, которая посредством своего нахождения «на границах» легко подвергается самопроизвольным изменениям и владеет противоречивостью. В-третьих, компьютерная информация и оставленные следы преступления легко подвержены уничтожению или изменению. На них довольно просто повлиять. В-четвертых, предметом и самой целью преступных действий в IT-сфере, а также непосредственным средством для их осуществления является информация и связанные с ней компоненты.

Для того чтобы классифицировать, нужно представить их в качестве самостоятельной группы преступлений, а уже внутри нее выделять подгруппы. Так, можно обозначить соответствующие подгруппы:

1. «Специальные составы гл. 28 УК РФ, групповым объектом которых являются отношения в сфере компьютерной информации. Они представляют собой преступления, непосредственно посягающие на данную сферу общественных отношений.

2. Преступления, предметом которых в том или ином статусе объекта гражданских правоотношений выступает информация и ее носители. К этому виду IT-преступлений относятся те, которые связаны с нарушением режима охраняемых законом тайн, нарушением авторских и смежных прав, неправомерным оборотом средств платежей, а также преступления в сфере оборота порнографии.

3. Преступления, объективная сторона которых включает действия, связанные с искажением информации. Примерами таких преступных деяний являются фальсификация единого государственного реестра юридических лиц, реестра владельцев ценных бумаг или системы депозитарного учета, фальсификация финансовых документов учета и отчетности финансовой организации и др.

4. Преступления, объективная сторона которых включает действия, связанные с передачей и распространением информации. Сюда относится клевета, публичные призывы к осуществлению террористической или экстремистской

деятельности, возбуждение ненависти либо вражды, а равно унижение человеческого достоинства и др.

5. Преступления, способ которых может включать или с обязательностью включает использование информационных технологий».

Однако есть и другие классификации видов преступлений, совершаемых с использованием компьютерных технологий. Так, например, можно рассмотреть конкретно 28 главу УК РФ, которая выделяет три вида подобных преступлений:

1. Неправомерный доступ к компьютерной информации.

2. Создание, использование и распространение вредоносных компьютерных программ.

3. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

1.3. Динамика распространения IT-преступлений в России и мире

Для того, чтобы понять всю суть преступлений в сфере компьютерных технологий, необходимо проследить их действие и распространение в динамике. Если проанализировать последние годы относительно уровня киберпреступности, можно понять некую систему развития данной преступной деятельности и разобраться с ее активностью [92].

Есть возможность рассматривать статистику на различных уровнях: и на мировом, и на российском, и на уровне субъектов РФ. Мы определим, что динамика киберпреступности нестабильна. Происходит постоянный рост с некоторыми спадами и подъемами, что отражено на рисунке 1 [92].

Графики и мирового уровня, и уровня России схожи и идут практически по одной линии, что показывает общий уровень развития и прогрессирования данного вида преступности. Однако следует остановиться на одном государстве, Российской Федерации, и изучить динамику распространения IT-преступлений.

Рисунок 1. Динамика изменения среднего числа атак на организации в неделю в России и в мире за первое полугодие 2020 года

Так, следует начать с 2019 года. За первые восемь месяцев в России установлено 180153 зарегистрированных преступлений в сфере информационных и компьютерных технологий [92]. Анализ позволил установить, что данное число на 66,8% больше, чем за аналогичный период предыдущего года.

Считается, что рост киберпреступности протекает весьма быстро и существенно. Это важно осознавать, потому что, по сравнению с другими видами преступных действий, противозаконные движения в сфере IT наиболее популярны.

Однако другие преступные действия, упомянутые ранее, тоже имеют свою динамику. Так, например, число тяжких преступлений увеличилось всего на 16,7%, а количество краж возросло на 3,5%. В свою очередь, особо тяжкие преступления стали совершаться на 3,1% меньше. Количество грабежей уменьшило свое число на 7,9%, а количество разбоев – на 8,9%. Даже число преступлений в сфере незаконного оборота наркотических средств, набирающих популярность в последнее десятилетие, стало меньше на 3,4% [92].

Да, несомненно, есть и те преступления, которые быстро растут и развиваются на одном уровне с киберпреступлениями. Это случаи мелкого хищения, посредничества во взяточничестве и дачи взятки, а также преступления коррупционной направленности. Однако при всем этом наибольший простор в своем современном обеспечении разнообразного порядка преступных действий имеет сфера преступлений, совершаемых с использованием компьютерных технологий.

В следующем 2020 году начальник главного организационно-аналитического управления Генпрокуратуры Андрей Некрасов заявил, что динамика преступлений, совершенных с использованием ИКТ или в сфере компьютерной информации, такова, что киберпреступность возрастает до немыслимых масштабов. Кроме того, с каждым годом становится все сложнее рас-

крывать дела по подобным преступлениям. Исходя из этого, можно даже опасаться угрозы национальной безопасности.

Еще в далеком 2015 году преступная деятельность в компьютерной и информационной сфере составляла меньше 2% случаев, а в 2020 – уже 25%. Так, 2020 год ознаменовался ростом киберпреступности на 73,4%. Всего зарегистрировано 510 300 преступлений, большая часть из которых осуществляется через сеть Интернет или при помощи телефонных устройств. Рост такого рода преступности происходил по всей стране, однако наибольший процент закреплен за Санкт-Петербургом и Ленинградской областью [92]. Все это связано с цифровизацией общественных отношений, а также с определяющими составляющими киберпространства: доступность информации, охват широкой аудитории, анонимность и трансграничный характер.

Кроме того, Следственный комитет отметил, что преступники приобретают все наиболее агрессивные черты [89]. Правонарушители умудряются находить новые способы сохранения анонимности и скрытия улик. Так, Краснов отмечает, что «бесконтактный и быстрый способ совершения» киберпреступлений превращает общество в слабое и уязвимое начало, к чему сотрудники правоохранительных органов не оказываются подготовленными [38, с. 10].

Если обратить внимание на уязвимость, то к этой категории очень точно относятся расчетные карты. Всего за один год количество их использования в криминальных целях увеличилось в 6 раз. Это подтверждает статистика МВД России [38, с. 11]. Кроме того, в два раза чаще стали использовать мобильные устройства. Также на 70 тысяч выросло количество краж с банковских счетов или электронных кошельков.

Что стало с российским государством и уровнем его правоохранительности? Для ответа на этот вопрос необходимо обратить внимание не только на преступную составляющую или статистику, но и на окружающие события в экономической и социальной жизни. Так, свое развитие получает пандемия коронавирусной инфекции. За счет того, что вводился карантин, весь мир как будто замирал. Вследствие этого вся жизнь переходила в компьютерную среду: и образование, и работа, и общение. Если раньше развитие технологий шло активными темпами, то в период пандемии заинтересованность в них мгновенно возросла. Не обошли эту заинтересованность и преступники. Правонарушители в сфере компьютерных и информационных технологий пытаются навязать людям мысль о том, что окружающие их вещи опасны, что все ноу-хау создаются против человеческой расы, а что тогда говорить о пандемии? Одни преступники уже практиковались в IT-сфере, другие только решились перейти в киберсреду, однако точно известно одно: киберпреступность резко увеличилась. Именно поэтому такую динамику многие ученые связывают с распространением болезни.

Так, 2020 год удивил сотрудников «Сбербанка» своим количеством жалоб. Более трех миллионов недовольных возгласов о том, что были произведены звонки от мошенников. Средства простых граждан активно стремятся похитить через мобильную связь. По мнению эксперта, «каждый 12-й звонок среднестатистическому россиянину является либо спамом, либо попыткой мошен-

ничества» [13, с. 124]. Происходят в некоторой степени атаки на обычных людей: фейковые звонки и рассылки со спамом, которые содержат поздравления о выигрыше или чем-то сострадательном. Людям предлагают перейти по ссылке или используют более простой способ: любыми методами пытаются вывести своего оппонента на ответ «Да». Очень многие люди замечают подобные мошеннические действия, стремящиеся нарушить покой государства и отдельно каждого.

2021 год показал статистику в использовании IT-технологий в каждом четвертом преступлении [92]. Однако при таком темпе рост количества подобных преступлений все же замедлился. Так, официальный представитель МВД России сообщила, что такие положительные результаты получены благодаря слаженной работе подразделений по раскрытию и расследованию преступлений в сфере высоких технологий. Сотрудники органов внутренних дел обучаются в специальных учреждениях, получают соответствующую квалификацию и знания для обращения с необходимой техникой. С помощью этого в правоохранительной системе наращивается потенциал в борьбе с ИТ-преступностью.

Однако преступления, совершаемые с использованием компьютерных технологий, продолжают совершаться. Так, например, пандемия в России способствовала тому, что IT-преступность выросла в 1,5 раза [48]. В основном, это мошенничество, кража и распространение наркотических средств. Под мошенничеством начальник Следственного департамента МВД РФ Лебедев, к слову, понимает «любые хищения, совершенные дистанционно, с использованием интернета, телефонной или иных видов связи» [92]. Это происходит по причине цифровизации общества и перехода организаций на электронные платформы.

В связи с этим появилась тенденция создания специализированных подразделений с отделами в каждом регионе. Однако несмотря на все усилия правоохранительной системы существуют факторы, не зависящие от нее и препятствующие расследованию.

К примеру, действительно важна максимальная скорость обмена информацией между правоохранительными органами и банковскими учреждениями, операторами сотовой связи, интернет-провайдерами. Нужно добиться наилучшего результата. Так, Центральному банку необходимо три дня для обнаружения необходимой информации, а в вопросах раскрытия преступлений важна оперативность.

1.4. Динамика судебных решений по делам в сфере совершения IT-преступлений

Сначала рассмотрим динамику судебных решений по делам в сфере компьютерных преступлений в России. Первый обвинительный приговор по статьям о компьютерных преступлениях был вынесен в Южно-Сахалинске 19 января 1997 года [90]. Студент института экономики, права и информатики занимался разработкой программы, нацеленной на подбор паролей к различным адресам

электронной почты. Кроме того, он занимался копированием информации из почтовых ящиков других людей. Данное преступление было раскрыто, и студенту присудили два года лишения свободы условно, а также штраф в 200 минимальных размеров оплаты труда.

Однозначно, были и те дела, которые закрывались в результате нарушения нескольких статей. Так, например, двое обвиняемых вступили в сговор, в результате чего один из них ввел в базу клиентов фирмы, в которой работал, фальсифицированные реквизиты. В итоге была получена продукция стоимостью более 70 тысяч рублей. Данное дело было возбуждено 6 февраля 1999 года. Одного из них осудили по статье 159 УК РФ (мошеничество), а второго, имеющего доступ к компьютеру, – по статьям 159 УК РФ и 272 УК РФ. Они получили 5 и 6 лет лишения свободы условно, соответственно [90].

А теперь проведем анализ судебной практики. Чтобы проследить динамику судебных решений, необходимо обратиться к проверенному источнику, каковым является сайт «Судебные и нормативные акты» [91].

Здесь возьмем конкретное число судебных решений с 2014 по 2019 год. За первый период (2014–2015) обозначим 120 уголовных дел, а за второй период (2018–2019) – 121 дело. Так, по представленному на сайте графику можно четко определить, что количество преступлений в 2019 в 26 раз больше, чем в 2013 году [91].

Наиболее часто встречается соотношение с 272 статьей УК РФ. Таких уголовных дел насчитывалось более 50%, то есть больше половины [91]. Статья же 273 УК РФ часто рассматривается в комплексе со ст. 146 УК РФ – нарушение авторских и смежных прав. Проведя анализ, мы видим, что подобные преступления совершались в меньшей степени (в пределах 37–41%).

Соответственно самыми малочисленными в своем распространении представляются те преступления, которые регулирует следующая статья – 274. Она встречается даже в соотношении 1%. Чуть больший процент у статьи 274.1 – неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации – около 3–4% [91].

Таким образом, обратившись к данным статистик, представленным на рисунке 2, которые подготовлены и распространены Генпрокуратурой [84], мы понимаем, что преступность в информационной и компьютерной среде продолжает расти. Это влечет за собой довольно неблагоприятные последствия для государства и общества.

Рисунок 2. Данные статистики Генпрокуратуры

Органам внутренних дел и обычным гражданам нужно объединить свои усилия и с максимальными усилиями приступить к ограничению возможностей для сообщества правонарушителей. Цель – добиться прогрессивной судебной статистики с раскрытыми уголовными делами и остановить рост такого вида преступности как киберпреступность.

Вопросы для самоконтроля:

1. Возможно ли объединить преступления, совершаемые с использованием информационно-коммуникационных технологий, по объекту уголовно-правовой охраны?
2. Как можно сформулировать понятие преступления, совершаемого с использованием ИКТ?
3. Присутствует ли в действующем Уголовном кодексе Российской Федерации понятие преступлений, совершенных с использованием информационно-телекоммуникационных технологий?
4. Почему, с Вашей точки зрения, преступления, совершенные с использованием информационно-телекоммуникационных технологий, в юридической литературе именуются по-разному?
5. Что составляет основу виртуального пространства?
6. В чем заключаются отличия информационных и компьютерных преступлений?
7. Как можно сформулировать понятие преступлений в сфере компьютерной информации?
8. В чем заключается киберпреступность?
9. Что относится к особенностям киберпреступлений?
10. Каким образом можно выделить подгруппы IT-преступлений?
11. Какие виды преступлений, совершаемых с использованием компьютерных технологий, выделяет УК РФ?

ГЛАВА 2.
ПРАВОВЫЕ АСПЕКТЫ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

2.1. Особенности законодательной базы противодействия преступлениям, связанным с IT-сферой

Российский законодатель пытается раскрыть проблемы, связанные с использованием Интернет, однако это удается довольно скудно. Информация в ГОСТ Р 56824-2015 [1] не позволяет раскрывать преступления в IT-сфере в полной мере. Существуют конкретные акты об информации и ее защите, а также некоторые федеральные законы, но они тоже не сильно влияют на продуктивность работы полиции.

Основным можно выделить Уголовный кодекс, который содержит статьи с прямой отсылкой к информационным преступлениям. Он регулирует их деятельность, накладывая санкции [4]. Так, обращаемся к главе 28 «Преступления в сфере компьютерной информации», содержащей статьи 272 «Неправомерный доступ к компьютерной информации», 273 «Создание, использование, распространение вредоносных программ», 274 «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети». Однако другие статьи тоже могут подходить под данную сферу преступной деятельности. Определяющим является практически любое отношение правонарушения к информационной среде.

Кроме того, следует указать на определенный список подобных нормативных правовых актов, регулирующих противодействие преступной деятельности в сфере ИТ:

- Конституция Российской Федерации (1993 г.);
- Концепция национальной безопасности Российской Федерации (2000 г.);
- Доктрина информационной безопасности Российской Федерации (2000 г.);
- ФЗ «О безопасности» (1993 г.);
- ФЗ «Об информации, информатизации и защите информации» (2006 г.);
- ФЗ «О государственной тайне» (1997 г.);
- ФЗ «Об участии в международном информационном обмене» (1996 г.);
- ФЗ «О лицензировании отдельных видов деятельности» (1998 г.);
- ФЗ «О связи» (1995 г.);
- ФЗ «Об электронной цифровой подписи (2002 г.).

Таким образом, правоприменение в области IT-преступлений довольно многогранно. Статьи по другим преступлениям могут применяться в информационной среде, однако это не значит, что отсутствует специальное узконаправленное законодательство. Существуют специфические федеральные законы, регулирующие конкретную сферу деятельности. В этом и заключается гибкость и особенность законодательной базы противодействия преступлениям, связанным с IT-сферой.

2.2. Квалифицирующие признаки преступлений, совершаемых с использованием информационно-телекоммуникационных технологий

При исследовании уголовно-правовой характеристики (квалифицирующих признаков) преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, наиболее важным в данном вопросе является исследование составов преступлений, предусмотренных УК РФ [4], которые прямо направлены на привлечение к уголовной ответственности виновных лиц за деяния, совершенные в глобальном информационном пространстве или с использованием информационно-телекоммуникационных технологий. В настоящее время раскрытие таких преступлений составляет практическую сложность. Именно поэтому предлагается обратить внимание на квалифицирующие признаки преступлений, совершаемых с использованием информационно-телекоммуникационных технологий.

В УК РФ закреплено несколько составов преступлений, объектом посягательства которых является компьютерная информация. В главе 28 УК РФ в настоящее время содержатся четыре состава преступлений, совершение которых направлено против компьютерной информации.

Сущность уголовно-правового запрета совершения неправомерных действий в отношении компьютерной информации состоит в том, что незаконный доступ к компьютерной информации недопустим, поскольку в результате получения доступа к компьютерной информации, в результате совершения неправомерных действий может быть уничтожена, утрачена компьютерная информация, в результате чего общественно опасным последствием станет нарушение деятельности различных систем государства: промышленности, обороны, связи и др.

Преступления в сфере компьютерной информации структурно располагаются в Разделе IX Уголовного кодекса Российской Федерации «Преступления против общественной безопасности и общественного порядка». В науке уголовного права родовой, видовой и непосредственный объекты составов преступлений определяются исходя из структурного закрепления соответствующего состава преступления в рамках раздела, главы и статьи, которые являются ориентиром для установления объекта уголовно-правовой охраны.

Родовым объектом преступлений, совершаемых в сфере компьютерной безопасности, являются общественные отношения, обеспечивающие общественную безопасность. В настоящее время законодатель оценивает, что преступления, совершаемые с использованием информационно-телекоммуникационных технологий, создают угрозу, прежде всего, общественной безопасности. Следует сказать, что применительно к виртуальному миру такая угроза носит не материальный, а виртуальный характер, но, вместе с тем, влечет реальные общественно опасные последствия.

Видовой объект преступлений, совершаемых в сфере компьютерной информации, можно определить на основе главы 28 УК РФ: это общественные отношения, складывающиеся в сфере обеспечения безопасности компьютерной информации.

Непосредственный объект преступлений, установленных главой 28 УК РФ, определяется из содержания конкретной статьи.

В ст. 272 УК РФ установлена уголовная ответственность за неправомерный доступ к компьютерной информации. Непосредственным объектом состава преступления, предусмотренного ст. 272 УК РФ, являются общественные отношения, обеспечивающие правомерный доступ к компьютерной информации. Основным непосредственным объектом состава преступления, предусмотренного ст. 273 УК РФ, являются общественные отношения, связанные с безопасным созданием, распространением и использованием компьютерных программ и компьютерной информации.

Преступления, расположенные в главе 28 УК РФ, объединяет объект преступного посягательства. Предметом этой группы преступлений является компьютерная информация. Неслучайно законодатель в Примечании к ст. 272 УК РФ легально закрепил определение компьютерной информации для дальнейшего ее использования в уголовно-правовом контексте. Согласно Примечанию 1 к ст. 272 УК РФ «под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи».

В юридической литературе компьютерная информация и ее определение являются предметом оживленных дискуссий. Авторами ставится под сомнение корректность изложенного законодательного определения компьютерной информации. Например, некоторые и вовсе не рассматривают в качестве предмета преступлений в сфере компьютерной информации компьютерную информацию, а пишут, что: «предметом преступного посягательства является не компьютерная информация, а информационная среда, связанная с созданием, преобразованием и потреблением информации».

По мнению А.В. Верещагиной, «предметом компьютерных преступлений с точки зрения российского законодательства является не просто компьютерная информация, а компьютерная информация, охраняемая законом» [32, с. 105]. С данным мнением трудно не согласиться. Если обратиться к диспозиции ст. 272 УК РФ, то можно увидеть, что в уголовном законе указана не просто компьютерная информация, а охраняемая информация. По нашему мнению, это свидетельствует о том, что предметом преступления является не любая компьютерная информация, а только информация ограниченного доступа.

В качестве дополнительного непосредственного объекта составов преступлений в сфере компьютерной информации можно выделить право на неприкосновенность частной жизни, иные законные интересы личности, общества и государства.

Деяния, составляющие элемент объективной стороны преступлений в сфере компьютерной информации, совершаются в форме активных действий.

Преступление, предусмотренное ст. 274 УК РФ, может быть совершено и путем бездействия.

Большинство преступлений в сфере компьютерной информации по конструкции объективной стороны являются материальными составами, что предполагает наличие трех элементов объективной стороны преступления: деяние, общественно опасные последствия и причинно-следственная связь между ними. Применительно к составу преступления, предусмотренному ст. 272 УК РФ, общественно опасные последствия выражаются в уничтожении, блокировании, модификации либо копировании компьютерной информации.

В ст. 274 УК РФ установлены аналогичные общественно-опасные последствия. Применительно к составу преступления, предусмотренному ст. 274.1 УК РФ, общественно опасные последствия могут выражаться также в нейтрализации средств защиты компьютерной информации. Исключением является состав преступления, предусмотренный ст. 273 УК РФ, который по конструкции объективной стороны является формальным составом преступления.

Наиболее дискуссионным вопросом, относящимся к объективной стороне преступлений в сфере компьютерной информации, является установление времени совершения преступления. Доминирующей является точка зрения, что временем совершения преступлений в сфере компьютерной информации, является момент нажатия на управляющую клавишу компьютера, запускающую конечную команду. Кроме того, промежуток времени от момента нажатия компьютерной клавиши до момента наступления общественно опасных последствий не влияет на квалификацию, поскольку на обработку команды может быть затрачено различное количество времени.

Что касается места совершения преступлений в сфере компьютерной информации, то применительно к данным составам преступлений местом совершения принято считать компьютерные сети. Также место совершения преступления и место наступления общественно опасных последствий зачастую не совпадают, поскольку, при совершении преступления в сети, общественно опасные последствия могут быть обнаружены на территории другого государства. Субъект преступлений в сфере компьютерной информации – общий, физическое вменяемое лицо, достигшее возраста 16 лет.

Преступления в сфере компьютерной информации могут быть совершены как умышленно, так и по неосторожности. Кроме того, для данной группы преступлений характерно наличие мотива: как правило, это корыстный мотив либо «интеллектуальный», то есть стремление виновного лица продемонстрировать свой профессионализм в сфере использования информационно-коммуникационных технологий.

Статья 273 УК РФ предусматривает ответственность за создание, распространение или использование компьютерных программ, предназначенных для несанкционированной модификации компьютерной информации или нейтрализации средств защиты информации. Субъективная сторона данного преступления закреплена в диспозиции статьи и предусматривает только такую форму вины, как умысел. Ответственность наступает в случаях, когда лицо осознавало общественную опасность своих действий, описанных в статье, равно как и

предвидело возможность или неизбежность наступления общественно опасных последствий и стремилось к их наступлению, а также если лицо осознавало общественную опасность своих действий в виде указанных деяний, предвидело возможность наступления общественно опасных последствий, не желало, но сознательно допускало эти последствия либо относилось к ним безразлично.

В ч. 2 ст. 273 УК РФ упоминается совершение данного преступления из корыстных побуждений. Мотив здесь имеет важное значение, и законодатель определил его как обязательный элемент субъективной стороны. Для установления этого элемента необходимо определить, что побудило лицо совершить данное преступление. Выявление мотива правонарушения необходимо для правильной квалификации преступления, а, следовательно, и для назначения наказания соответственно со степенью вины.

Статья 274 УК РФ предусматривает ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

Нарушение правил эксплуатации возможно только при неосторожной форме вины, по легкомыслию или небрежности. В данном преступлении важно установить причинно-следственную связь между деянием лица и результатом, повлекшим к уничтожению, блокированию, модификации или копированию компьютерной информации, причинившим крупный ущерб. Данные последствия не должны быть следствием сбоя программы или ошибки в работе компьютера.

Статья 274.1 закрепляет ответственность за создание, распространение и (или) использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации. Состав преступления введен 26 июля 2017 года.

Противоправные деяния, предусмотренные частью первой, предполагают прямой умысел. Законодатель определяет конкретные деяния и их последствия. Прямой умысел также предусматривается и в преступлении, описываемом во второй части статьи. Часть третья статьи 274.1 УК РФ содержит ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой информации. Уголовная ответственность за нарушение правил эксплуатации наступает только при неосторожной форме вины.

Наиболее распространенную группу преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, составляют преступления против собственности. Среди них: кража (ст. 158 УК РФ), мошенничество в сфере кредитования (ст. 159. 1 УК РФ), мошенничество с использованием электронных средств платежа (ст. 159.3 УК РФ), мошенничество в сфере компьютерной информации (ст. 159. 6 УК РФ), неправомерный доступ к компьютерной информации (ст. 272 УК РФ), создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ).

Согласно ч. 1 ст. 159.6 УК РФ, «мошенничество в сфере компьютерной информации, то есть хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств

хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей…». Указанной нормой установлена уголовная ответственность за мошенничество (хищение чужого имущества или приобретение права на чужое имущество), совершенное с использованием информационно-телекоммуникационных сетей или с использованием компьютерной информации. Мошенничество с использованием компьютерной информации действительно можно назвать современным преступлением, современным видом хищения, совершенным путем обмана.

Объективная сторона данного состава преступления заключается в незаконном проникновении в информационную среду и совершении хищения чужого имущества или прав на чужое имущество путем совершения различных операций с компьютерной информацией (ввод, удаление, модификация, блокирование), а также иного вмешательства в процессы хранения, обработки и передачи информации.

2.3. Особенности правового регулирования общественных отношений в IT-сфере

Опасность преступлений в виртуальном пространстве в последние годы возрастает во всем мире, с чем ведут борьбу правоохранительные органы, информируя граждан о возможных посягательствах, разработчики совершенствуют систему обеспечения информационной и компьютерной безопасности – в целом организуя единую систему противодействия преступлениям в сфере информационных технологий. Преступность в сфере кибернетики захватывает достаточно большой спектр. Увеличивается доля вероятности совершения посягательств на частную и государственную сферу деятельности. В связи с этим расширяется доля общественных отношений в IT-сфере, что влечет за собой необходимость совершенствования их правого регулирования.

Данную проблему активно исследовали многие ученые и правоведы. В частности, З.И. Хисамова отмечает, что современное состояние правового регулирования общественных отношений, связанных с определением основания и условий дифференциации уголовной ответственности за совершение преступлений с использованием ИКТ, является несостоятельным [54, с. 119]. Причиной тому выступает бессистемное регулирование указанных общественных отношений. С автором трудно не согласиться. Современное состояние преступности в информационной среде требует комплексного регулирования уголовной ответственности за совершение преступлений с использованием информационно-телекоммуникационных технологий.

Обобщив квалифицирующие признаки рассмотренных преступлений, сформулируем общие ***квалифицирующие признаки преступлений***, совершаемых с использованием информационно-телекоммуникационных технологий.

Преступления, совершаемые с использованием ИКТ в сфере компьютерной информации, посягают на общественную безопасность. Преступления, совершаемые с использованием информационно-телекоммуникационных технологий, направлены на дестабилизацию нормального уровня личной, общественной и государственной безопасности. Общественные отношения, обеспечивающие нормальный уровень безопасности личности, общества и государства, являются основным непосредственным объектом преступлений, совершаемых с использованием ИКТ. В качестве дополнительного объекта преступного посягательства можно выделить права и законные интересы личности, общества и государства, такие как права на неприкосновенность частной жизни, тайны, личной переписки и др.

Кроме того, в качестве дополнительного объекта преступного посягательства можно выделить право собственности. В том случае, если информационно-телекоммуникационные технологии являются способом совершения преступления, а умысел виновного лица направлен на хищение чужого имущества путем использования информационно-телекоммуникационных технологий, основным непосредственным объектом преступления следует признавать право собственности, а в качестве дополнительного объекта выделять общественные отношения в сфере общественной безопасности.

Объективная сторона преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, может быть выражена как в форме действия, так и бездействия. Представляется, что в преобладающем числе случаев преобладает активная форма совершения преступлений с использованием информационно-телекоммуникационных технологий. Для совершения преступления в активной форме виновному лицу необходимо совершить ряд определенных действий, используя информационно-телекоммуникационные технологии, которые приведут к преступному результату.

Преступления в сфере информационно-телекоммуникационных технологий в пассивной форме могут иметь место в том случае, если виновное лицо в силу определенных обстоятельств может совершить действия, не приводящие к нарушению общественной безопасности, но в силу бездействия виновного лица наступают общественно опасные последствия.

По форме вины преступления, совершаемые с использованием информационно-телекоммуникационных технологий, являются умышленными, поскольку виновное лицо осознает общественную опасность своего деяния, предвидит возможность или неизбежность наступления общественно опасных последствий, выражающихся в причинении вреда общественной безопасности, желает их наступления либо не желает наступления общественно опасных последствий, но сознательно допускает их наступление.

Мотив и цель совершения преступлений с использованием информационно-телекоммуникационных технологий не влияют на правильность квалификации и не устанавливаются законодателем в качестве обязательных признаков субъективной стороны преступления. Однако большинство преступлений совершаются из корыстной заинтересованности.

Анализ действующего законодательства позволяет сделать вывод, что субъект преступлений, совершаемых с использованием ИКТ, является общим, то есть физическое вменяемое лицо, достигшее шестнадцатилетнего возраста.

В настоящее время одним из актуальных вопросов совершенствования уголовной ответственности за преступления, совершаемые с использованием ИКТ, является приведение в соответствие уголовного закона современным возможностям совершения преступлений с использованием информационно-телекоммуникационных технологий.

Эффективность противодействия преступности в сфере ИКТ возможна, в первую очередь, за счет совершенствования уголовно-правовых запретов. В частности, актуализируется проблема изменения диспозиций ряда уголовно-правовых норм с целью детализации способа совершения преступлений против собственности путем прямого указания на использование при совершении преступлений информационно-телекоммуникационных технологий.

Таким образом, например, такой квалифицирующий признак как использование информационно-телекоммуникационных технологий при совершении мошенничества позволит детализировать способ совершения преступлений. Данный квалифицирующий признак может быть предусмотрен в диспозиции ряда уже «традиционных» преступлений.

Также следует ответить на вопрос, какое место использование ИКТ должно занять в сложившейся системе дифференциации уголовной ответственности? Однако представляется, что в настоящее время будет сложно ответить на этот вопрос, поскольку законодатель не пришел к определенности по вопросу этимологизации преступлений, совершаемых с использованием информационно-телекоммуникационных технологий. Подтверждением тому является наличие в уголовном законе преступлений, для которых компьютерная информация является дополнительным объектом посягательства (преступления против собственности) и преступления, для которых компьютерная информация является основным непосредственным объектом преступления (глава 28 УК РФ).

Отсутствие со стороны законодателя четкой типологизации преступлений, совершаемых с использованием ИКТ, затрудняет и вопрос о выделении квалифицирующих признаков таких преступлений.

Вопросы для самоконтроля:

1. Какие нормативные акты можно отнести к сфере защиты информации?
2. Какие федеральные законы РФ относятся к сфере защиты информации?
3. В рамках каких статей УК РФ содержит прямые отсылки к информационным преступлениям?
4. Какие составы преступлений содержит глава 28 УК РФ?
5. В чем состоит сущность уголовно-правового запрета совершения неправомерных действий в отношении компьютерной информации?
6. Исходя из чего науке уголовного права определяются родовой, видовой и непосредственный объекты составов преступлений?
7. Что является родовым объектом преступлений, совершаемых в сфере компьютерной безопасности?
8. Что является видовым объектом преступлений, совершаемых в сфере компьютерной информации?
9. Как определяется непосредственный объект преступлений, установленных главой 28 УК РФ?
10. За что устанавливает уголовную ответственность ст. 272 УК РФ?
11. Что объединяет преступления, описанные в главе 28 УК РФ?
12. Какие подходы к понятию компьютерной информации существуют в юридической литературе?
13. Что является предметом компьютерных преступлений с точки зрения российского законодательства?
14. Что является наиболее дискуссионным вопросом, относящимся к объективной стороне преступлений в сфере компьютерной информации?
15. В чем заключаются особенности правового регулирования общественных отношений в IT-сфере?

ГЛАВА 3.
МЕРОПРИЯТИЯ ПО ПРОТИВОДЕЙСТВИЮ ПРЕСТУПНОСТИ В СФЕРЕ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

3.1. Особенности способов раскрытия преступлений, совершаемых с помощью информационных технологий

Важно понимать, что IT-преступления предполагают анонимизацию личности правонарушителя. С помощью дистанционности совершения преступлений человек не показывает свое лицо, не оставляет отпечатков пальцев, волос или частичек кожи – ничего. За счет наличия такого посредника, как компьютер, личность преступника довольно тяжело раскрыть. Следует отметить, что эта проблема является следствием отсутствия систематизированных данных (информационных систем) о лицах, сетевых URL-адресах, учетных записях, ник-неймах в сети Интернет, которые проходили или проходят по оперативным материалам в качестве объектов оперативной заинтересованности или их связей.

Облегчить раскрытие личности может помочь, например, сочетание проведения оперативно-поисковых мероприятий в информационном пространстве сети Интернет и создания соответствующих информационных ресурсов. Так будет собираться больше количество непосредственной информации. В этой связи свое мнение высказывает О.П. Грибунов, который точно уверен, что в настоящее время без современных технологий процесс раскрытия и расследования преступлений уже практически невозможен. Кроме того, анализ практики показал, что сотрудники оперативных подразделений ОВД в основном пользуются лишь исходными данными, полученными в ходе оперативно-разыскных мероприятий. Это могут быть URL-адреса ресурсов в сети Интернет, никнеймы, брендовые названия интернет-площадок, наименования тематических форумов и т.д. Однако все прекрасно понимают, что Интернет – огромная сеть. Внутри нее прячется бесконечное количество и ник-неймов, и форумов. Информационное пространство хранит большое количество данных, которые трудно связать с конкретным преступлением.

Раннее было сказано, что преступник через дистанционность не оставляет ничего. Это не совсем так. Не остаются материальные, физические следы, а вот как раз цифровые остаются. Любое действие в Интернете сохраняется в виде малюсенького виртуального атома среди огромных сетей [37, с. 255]. Так, преступники, стараясь избежать своей деанонимизации, постоянно меняют никнеймы, названия интернет-площадок и форумов. В результате таких действий происходит то, что у сотрудников ОВД создается иллюзия о все большем заполнении IT-пространства новыми правонарушителями.

Что же тогда делается для раскрытия таких преступников? Существует такое понятие, как «почерк». Это конкретная модель поведения при совершении своих действий. Почерк – то, что выделяет одного преступника среди мил-

лиона других. При этом почерк может быть оставлен как специально самим преступником, так и случайно за счет своих привычных действий.

Например, при совершении серии убийств преступник может отрезать своим жертвам указательный палец на правой руке. Это относится к первому варианту, специально. Для чего? Может быть, убийце нравится «играть» с полицейскими, давить на нервную систему и заставлять всех бояться за счет своей же смелости. Именно с помощью такой индивидуализации появляется возможность раскрывать преступления, тем более в масштабном объеме. Так и преступления, совершаемые с использованием ИТ, доказывают, что каждому преступнику в сети Интернет присущ определенный «почерк» [52, с. 134].

Так как киберпреступность все больше распространяется, необходимо принимать соответствующие меры [76]. В Следственном комитете создается «специализированный отдел по расследованию преступлений, совершенных с использованием высоких технологий. Вновь созданное подразделение должно стать площадкой, объединяющей усилия различных государственных ведомств, научных учреждений и специалистов для эффективного и слаженного противодействия преступным явлениям в информационной сфере» [49].

Следователь данного отдела должен не только сосредотачиваться на процессуальных действиях, но обращать внимание на конструирование специальных подходов к следственным действиям и методик соответствующего производства [89]. Кроме того, важно тщательно разработать аналитическую базу для аккумулирования сведений о совершенных преступлениях в сфере IT-технологий.

Однако одним из препятствий на пути к достижению такой важной цели, как увеличение эффективности расследования, является несвоевременное обращение в компетентные правоохранительные органы. Чтобы сотрудники органов внутренних дел могли взяться за соответствующее дело, им необходима информация, которая запрашивается у граждан.

Они же, в свою очередь, для возможности предоставления сведений, используют системы логирования: хранение информации об адресах, различных перемещениях данных. Такие системы помогают узнать, кто и когда заходит на сайт, какими средствами пользуется, и другое. Данные сведения воспроизводят линию действий правонарушителя, отражая весь его преступный замысел.

При этом обычным гражданам важно помнить, что им тоже необходимо контролировать все действия, ими совершенные. Так, хищение денежных средств с помощью телефонных и компьютерных средств нужно запросить и забрать выписку из своего банка с подтверждением факта перевода денежных средств и указанием реквизитов получателя.

Необходимо запомнить и воспроизвести как можно больше полезной информации: адрес электронной почты, номер телефона, а, возможно, и адрес офиса правонарушителя. Кроме того, очень важным действием будет звонок в банк и его оповещение о случившемся. Чем раньше это будет сделано, тем больше шансов, что банк сможет оказать содействие своему клиенту при расследовании дела. Почему это все имеет значение? Действия пострадавшего, на-

целенные на содействие органам внутренних дел, способствуют наиболее оперативному процессу принятия соответствующих мер.

Заметим, что самым плодоносным из всех вариантов является профилактика. Если вести здоровый образ жизни, то не придется пить лекарства и страдать от недомогания. Так и со сферой преступности. Чтобы не стать жертвой преступников в сфере IT-технологий, необходимо изучать алгоритмы действий при взаимодействии с правоохранительными органами, а также применять соответствующие превентивные меры, то есть предупреждающие и предохранительные [89].

Обращаясь к рисунку 3 [78], мы видим те меры предосторожности, которые должны использовать. Данные действия с большой вероятностью предостерегут от перехода в статус жертвы преступления. Так, необходимо использовать антивирусные программы, устанавливать сложные пароли, включающие не только цифры, но и буквы, знаки. Пароль в виде даты рождения или повторяющихся «1» – наихудший вариант для обеспечения безопасности аккаунтов. Если тщательно подойти к выбору защиты своих данных, то преступникам будет сложнее переходить по ссылкам с целью получения информации.

Кроме того, например, необходимо тщательно выбирать ту информацию, которую человек собирается распространять через информационное пространство, передавать каким-либо лицам и размещать в социальных сетях [44, с. 52; 45, с. 100; 46, с. 54]. По статистике, 90% утечек информации происходит из-за неосторожных и необдуманных действий субъектов персональных данных, то есть по их же вине.

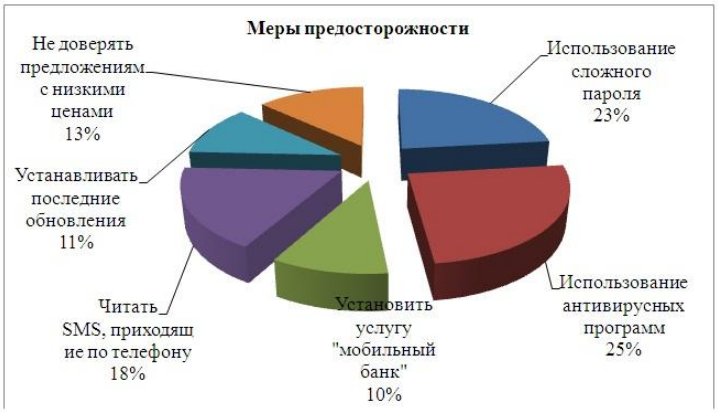

Рисунок 3. Киберпреступность глазами студентов
Амурского колледжа строительства и жилищно-коммунального хозяйства

Именно поэтому и сотрудникам органов внутренних дел, и обычным гражданам нужно очень внимательно относиться к таким нюансам [56, с. 268]. Важно проводить тщательную профилактику, более внимательно относиться к распространяемым данным и всеми силами пытаться уменьшить количество таких преступлений.

3.2. Меры по противодействию преступлениям в сети Интернет

Технологический прогресс прочно внедрился в нашу повседневную жизнь и стал неотделимой частью современного общества. Информация заполонила весь виртуальный мир, создавая избыток данных [15, с. 103]. Очень часто приходится сталкиваться с информацией аморального характера, которая содержит в себе всевозможные варианты отклоняющегося восприятия мира. Данной деятельностью занимаются как отдельные преступные элементы, так и целые сообщества, которые реализуют в сугубо личных интересах экономическую или иную выгоду, вовлекая в деятельность теневого характера неподготовленных людей [12, с. 104].

Что можно сказать о преступлениях, совершенных с помощью сети Интернет и какие мероприятия проводятся по реализации противодействия со стороны ведомства МВД?

В настоящий момент совершение преступлений через сеть Интернет чрезвычайно возросло. По статистическим данным МВД России в 2021 году было совершено 212 674 преступлений с использованием компьютерных и телекоммуникационных технологий, что составляет 43,8% от общего количества совершенных преступлений.

Частым видом преступлений являются те, которые носят характер легкой доступности. Они заманивают аудиторию, которая не владеет навыками распознавания лживой информации, направленной на запугивание и введение в заблуждение людей. Контент, публикуемый на просторах сети Интернет, ставит под угрозу обмана все общество, которое не умеет на профессиональном уровне работать с информацией и владеть навыками самоконтроля. Ведь очень часто преступления осуществляются под давлением на человеческую психологию. Среди данной категории выделяются следующие: нарушение авторских прав, распространение запрещенной информации, пропаганда экстремизма, мошеннические действия, незаконный доступ к данным, взлом серверов, киберпреступления и другие [30, с. 41].

Самым распространенным преступлением в Интернете являются ***виртуальные хищения***. Именно в сфере информационных технологий хищение развилось достаточно хорошо и поэтому имеет множество видов. Преступники создают различные схемы обмана в большинстве случаев с последующей экономической выгодой, пытаясь обойти рамки закона и надзора со стороны специализированных органов.

Многообразие информации усложняет пользовательскую деятельность в сети Интернет. Появляется многообразие незнакомых терминов, формулировок, доменов. Одной из разновидностей хищений выделяют «***кардинг»*** – это хищение средств через банковские операции, совершаемые незаконным путем, методы которых вводят пользователя в заблуждение, чтобы завладеть его базой данных [24, с. 111]. Доступ к пользовательским данным очень прост, вся информация может содержаться на аккаунте интернет-магазина, где хранятся банковские, паспортные и иные конфиденциальные данные для личного поль-

зования – оплаты и доставки покупок. В свою очередь злоумышленник может воспользоваться этим [33, с. 129].

Иная разновидность преступления «***фишинг***» – это преступное деяние, которое предполагает ложное уведомление от банка о всевозможных внутрибанковских операциях с получением пароля. В данных уведомлениях чаще всего просят перейти по ссылке для последующих целенаправленных действий, которые носят характер смены пароля, ввода и последующей утечки данных через подложные домены, и подобных задач, тем самым получая конфиденциальные данные пользователя [35, с. 23].

Задачей данной преступной деятельности является доступ к персональным данным, личным счетам и иным серверам, которые стоят под угрозой взлома. Для реализации своей преступной деятельности мошенники используют «кардинг» или «фишинг». Два данных термина могут быть не понятны определенной прослойке информационного общества, поэтому немаловажным является получение информационной грамотности, в первую очередь, чтобы обезопасить себя от всевозможных посягательств.

Противодействие данным видам преступлений должно осуществляться напрямую от источника. Тем самым необходимо обеспечить более сложное шифрование серверов, использование лицензированных антивирусных программ, которые будут блокировать сайты злоумышленников с целью более затрудненного доступа к данным и фиксацией о них с внесением в базу ОВД информационной безопасности для пресечения информационных преступных посягательств.

Самым простым способом совершения хищения и получения незаконного доступа к данным лица является метод «***клонирования***». Самым наглядным примером является подмена одного символа на схожий знак. Существует электронный кошелек «Qiwi» для совершения денежных операций и хранения средств.

Злоумышленники в своих уведомлениях или сообщениях, присылая ссылку подложного сайта, меняют несколько символов, предоставляя подложный сайт, содержащий вредоносную программу. Настоящая ссылка данной электронной системы выглядит так: www.qiwi.ru, а ссылка злоумышленника будет выглядеть таким образом: www.qivi.ru. Перейдя по ней, пользователь обречен на утечку данных [8, с. 105].

Противодействие данным видам преступлений должно осуществляться, в частности, и системой безопасности устройства. В современных гаджетах установленны специализированные программные обеспечения, распознающие ложные сервера, с предупреждением о краже данных – это своевременно информирует пользователя о возможной угрозе. Данная сфера в настоящее время прогрессивнее защищена при эксплуатации программ антивирусного и мониторингового характера. Более разработанными антивирусными программами являются: Avast, Антивирус Касперского, Agnitum, которые осуществляют защиту устройств. Попытки взлома также должны отправляться на сервера ОВД по информационной безопасности с целью отслеживания и пресечения преступных действий и атак.

Многочисленные преступления в современном мире совершаются посредством бесконтактной оплаты NFS, которая осуществляет функцию дистанционного соединения платежного аппарата и карты или же смартфона с установленным приложением. Данная программа значительно облегчает способ расчета при совершении оплат в магазинах. С одной стороны, все технологии созданы во благо человеку, но, с другой стороны, данное благо оборачивается массовым бедствием для обычных пользователей, которые и становятся жертвами преступников.

Функционал данной системы слабо защищен. В настоящее время доступна функция установки лимита бесконтактным методом, чтобы обезопасить себя от нежелательных списаний денежных средств и стать жертвой преступника.

Преступные элементы общества используют приборы – «перехватчики», которые устанавливают соединение с последующим списанием денежных средств на офшорные счета, которых нет в национальной базе данных. Данная технология усложняет систему выявления преступников, потому что практически невозможно установить факт несанкционного соединения через систему безопасности. Единственное оружие – это бдительность человека.

Немаловажной проблемой в противодействии данным преступлениям будет являться умение вовремя и безошибочно противостоять возможной угрозе. Большинство людей не понимают, как необходимо себя вести и какие меры предпринимать для блокировки взлома системы. Основной задачей ОВД является проведение с гражданами работ по противодействию преступности в информационной среде, что снизит уровень пострадавших от данных деяний.

Одним из самых простых методов, который поможет обезопасить себя от нежелательных списаний средств, – это алюминиевый чехол, который экранирует гаджет от воздействия электромагнитных волн и препятствует сбою в системе банка, тем самым защищая все средства. Но ничто так не заменит в обеспечении безопасности, как собственная бдительность. Очень часто жертвы преступников сами идут на контакт, сообщая свои конфиденциальные данные заведомо ложным сотрудникам банка или ОВД. Граждане не проверяют истинность оглашаемой им информации и попадают на крючок к злоумышленнику.

Противодействие данному виду преступлений на современном этапе разработок находится на стадии зарождения, так как система бесконтактных платежей стала новеллой, а система безопасности не действует целеполагающим образом, оставаясь практически незащищенной как со стороны ОВД, так и программного обеспечения.

Единственным доступным способом защиты граждан от злоумышленников является информирование, что часто проводится сотрудниками ОВД, призывая граждан к повышению бдительности с целью обезопасить себя от неприятных последствий.

Переход на новый этап развития в обществе, касаемо бесконтактных оплат, о которых раньше нельзя было подумать, стало повседневной реальностью. Информатизация берет стабильный рост и развитие, но вместе с этим должна развиваться и безопасность пользователей. Без обеспеченной безопасности людям будем не выгодно и даже очень убыточно пользоваться незащищенной сис-

темой. Как известно, с появлением новшеств всегда появляются в данной сфере преступники, которые пытаются всячески навредить ради своей выгоды и остаться безнаказанными [10, с. 35].

На данный момент ведется усиленная разработка программных обеспечений, антивирусных устройств, которые будут эффективным способом противодействовать взлому персональной системы граждан, тем самым снижая уровень преступности в сети Интернет.

Таким образом, главная задача МВД в современном мире – предотвратить экономическую киберпреступность с помощью усовершенствования программного обеспечения, внедряя ее в структурные подразделения ОВД, которые смогут отслеживать мошеннические действия, киберпреступления, взлом серверов и оперативно их ликвидировать с использованием информационной системы безопасности. Чтобы обеспечить максимальную гарантию безопасности, необходимо провести переустановку драйверов и серверов устройств, которые смогут изначально блокировать подозрительные сайты, через которые осуществляется преступная деятельность.

3.3. Противодействие информационной преступности в социальных сетях

В современном мире в период информатизации общества, которое переместилось в глобальную сеть Интернет, появилось такое понятие, как социальная сеть. Социальная сеть – это место общения, обмена информацией, любыми данными, содержащимися в любом формате (текст, аудио, видео), предназначенное для дистанционного контакта с другим пользователем. Социальные сети стали одной из частей современного мира, что также упростило процесс коммуникации и обмена информацией [10, с. 24].

Передача необходимой информации осуществляется в течение секунды, даже если человек находится на другом конце планеты. Существуют и на данный момент успешно функционируют такие мессенджеры, как: российские сети «ВКонтакте» и «Одноклассники», а также американские: Instagram, Facebook и Twitter. В 2022 году данные сети подверглись блокировке по Указу Президента Российской Федерации в связи с международной обстановкой и вводимыми санкциями. Подобными средствами обмена информацией являются Viber и WhatsApp. Они также находятся в зоне риска по блокировке серверов, поскольку являются небезопасными для использования. Очень часто сливаются данные пользователей, которые используются для реализации преступных действий [41, с. 30].

Социальные сети стали виртуальным миром, в котором общаются и обмениваются разного рода информацией все люди. Достаточно трудно представить современного человека, который не пользуется различными мессенджерами, так как они достаточно быстро вошли в нашу повседневную жизнь и упростили ее. Но усложняет использование социальных сетей появление преступности, а для

противодействия необходимо международное соглашение: только совместными усилиями со стороны государств можно достичь желаемого результата.

Специализированными и высококвалифицированными специалистами в настоящее время проводится разработка новых программ по противодействию преступности в сети Интернет. Также немаловажным является привлечение иностранных специалистов, заинтересованных данной деятельностью. Обмен опытом в новой среде коммуникаций и новшеств – это очень ценный фактор, способствующий информационному прогрессу и появлению новых методов защиты.

В глобальном масштабе контроль над социальными сетями возможен, но для этого требуется много инвестиций и международное соглашение о сотрудничестве. Каждое государство в разной степени развито в сфере информационных технологий, что не позволяет некоторым странам должным образом защитить себя от преступных посягательств. Для защиты общества и всех государств необходима выработка единой системы противодействия преступности с использованием программного обеспечения.

Выработка навыков противодействия преступности в социальных сетях будет способствовать стабильному развитию государств, уменьшению количества преступности, повышению качества жизни, так как совершаемые посягательства наносят немалый ущерб социуму. Основная проблема XXI века – это борьба с интернет-преступностью.

Наибольшее количество преступных посягательств замечено со стороны украинских граждан в российских социальных сетях. Мониторинг со стороны органов внутренних дел, а также пресечение противоправных деяний значительно затрудняется в силу враждебных отношений между Россией и Украиной. Вести борьбу с этим позволит только ограничение доступа российских социальных сетей на враждебных территориях.

Немалое количество преступлений с использованием социальных сетей составляют общественно опасные деяния, связанные с ***незаконным оборотом наркотических веществ***. Наркооборот растет в геометрической прогрессии благодаря сети Интернет, где можно создать анонимный аккаунт и распространять необходимые сведения и данные о сбыте и распространении. Но специализированные службы достаточно быстро вычисляют данные аккаунты и пробивают их местоположение по IP-адресу, проводя мониторинговые действия за преступными элементами.

Противодействие данным видам преступлений осуществляется путем мониторинга социальных сетей специальными подразделениями ФСБ совместно с МВД. Существует определенное программное обеспечение – база терминов автоматического считывания, использование которых заносит id-аккаунт пользователя в систему контроля. В последующем специальными органами осуществляется анонимный надзор за активностью аккаунтов, вычисление владельцев, наблюдение за их деятельностью и пресечение преступных деяний с помощью социальных сетей.

Самый распространенный метод продвижения противоправных операций с наркотическими веществами – совершаются через социальную сеть «ВКонтакте» – 81%. Именно поэтому социальные сети стали подведомственны специальным службам и подверглись внедрению новых программ мониторинга.

Второе место по совершению преступных посягательств занимают деяния, направленные на ***частную собственность***. Самым распространенным методом преступности являются мошеннические действия. С использованием социальных сетей совершаются кражи путем обмана при отсутствии признаков хищения. Фактически происходит, что жертва сама переводит средства на счета злоумышленников, находящихся в офшорах, которые очень трудно отследить и пресечь противоправные деяния.

Противодействие данным видам преступлений находится на стадии становления, так как развитие информатизации происходит очень интенсивно, а разработка методов противодействия должна базироваться на вариантах посягательств, которые очень сложно предсказать, чтобы организовать методы противодействия. В настоящее время ведутся глобальные разработки программных инструментов, которые обезопасят пользователей от преступных посягательств. Пока лишь человеческая бдительность и здравый разум могут его предостеречь от нежелательных последствий.

Особое внимание отводится публикуемым мошенниками объявлениям на выгодных условиях предоставить товары и услуги, что непосредственно является ловушкой для овладения денежными средствами потерпевшего. Мошенники публикуют заведомо ложные объявления о продаже авиабилетов по низким ценам, сдаче квартиры в аренду и другие заманчивые предложения.

Иной разновидностью преступления является вымогательство методом ***шантажа***. Жертва попадает на уловку преступника, который угрожает распространением сведений, позорящих потерпевшего. Практически всегда данный способ реализуется незаконным доступом к диалогам, тем самым, нарушается конституционное право гражданина на тайну личной переписки. Посредством этого совершается вымогательство с угрозой о неприятных последствиях в случае невыполнения условий или обращения в правоохранительные органы.

Противодействие данным видам преступлений осуществляется методом дополнительного шифрования своих данных и затрудненного доступа к ним. Система безопасности практически каждого приложения имеет двухфазную установку пароля, что говорит о развитии и новшестве программных обеспечений. На стадии внедрения находится программное обеспечение, открывающее доступ только по данным дактилоскопии, которые проблематично подделать.

Все цели в современном информационном обществе направлены на безопасное использование глобальной сети Интернет, создавая необходимые программы по обеспечению противодействия посягательствам на личную жизнь граждан.

В перечисленных категориях преступлений наибольшую долю составляют деяния, связанные с распространением экстремистских материалов в социальных сетях.

Распространение экстремистской информации осуществляется в форме видеоматериала. Также информация экстремистской направленности может быть представлена в виде текста, графических изображений и аудиофайлов.

Было выявлено немало преступлений, связанных с нарушением порядка выдачи и оборота официальных документов. С использованием групп в социальных сетях осуществлялся сбыт листков нетрудоспособности, поддельных документов о высшем образовании, поддельных водительских удостоверений.

Для совершения противозаконных действий активно используются социальные сети. Преобладает количество общественно опасных деяний при помощи социальной сети «ВКонтакте». Нередко упоминаются такие социальные сети, как «Одноклассники», «Мой Мир@Mail.ru», «Друг вокруг» и Skype.

Таким образом, можно подвести итог, что в современном мире с появлением социальных сетей – виртуальной реальности, которая заменила повседневную жизнь, появляются новые виды информационных преступлений, с которыми достаточно сложно вести борьбу. Идет разработка новых усовершенствованных программных инструментариев, систем безопасности сайтов, в том числе антивирусных программ, помогающих распознавать нестандартные материалы и веб-сайты, блокируя их и закрывая доступ, делая виртуальное пространство более удобным и безопасными.

3.4. Мероприятия по противодействию киберпреступности

Киберперступность стала основной угрозой для информационного пространства. С целью эффективного противодействия киберугрозам необходима стратегия взаимодействия в сфере кибербезопасности, способная защитить как государство, так и его граждан, создавая реализуемые методы противодействия различным видам информационных преступлений.

Мир живет в эпоху, когда информационные технологии и кибермир стали неотъемлемой частью общества и каждого индивида в отдельности. Кибермир предоставляет огромные возможности для упрощения и улучшения всей жизнедеятельности человечества, но в связи с этим появилось многообразие новых видов преступлений, с которыми необходимо вести активную и постоянную борьбу.

Стремительное развитие информационных технологий и информатизации общества привело к появлению новых видов преступлений и угроз - таких, как киберпреступность, кибертерроризм, кибервойна. Массовые атаки Интернет-угроз могут нанести масштабный вред как обществу, так и всему государству в целом. Нередко были замечены кибератаки со стороны враждующих сторон – США и Украины в отношении Российской Федерации. Их целью является задача взлома системы безопасности и попытки получить доступ к ней. К счастью, сделать этого не удалось.

Киберпреступность более многостороннее явление, нежели «компьютерная преступность», и такое многообразнее отражает природу данного феноме-

на. Характерной особенностью кибертерроризма и его отличиями от киберпреступности выступают его масштаб, интенсивность, открытость и тяжесть последствия.

Кибертерроризм – это серьезная угроза человечеству, сравнимая с оружием массового поражения. Эта же угроза может исходить как от террористических, так и от экстремистских организаций, в том числе от некоторых спецслужб, стоящих за ними, которые стремятся реализовать геополитические амбиции своих руководителей в сети Интернет.

Так, по мнению некоторых ученых, кибертерроризм является более опасным видом терроризма, чем биологический или химический терроризм, так как может угрожать миллионам людей из-за уязвимости военных компьютеров. Именно поэтому в современном мире пристальное внимание уделяется информационной среде, как неотъемлемой части нашего современного общества.

В оперативном искусстве и тактике за последние десятилетия произошли принципиальные перемены, которые требуют от государств радикального пересмотра прежних военных доктрин и критической переоценки всего спектра областей военного искусства. По сути дела, сегодня речь идет уже о появлении нового военного искусства, когда прежние оценки, опыт и знания требуют радикального пересмотра, либо даже отказа от прежних взглядов.

В силу разного рода причин все труднее становится отделить военную и кибербезопасность одного государства, региона от других государств, что неизбежно ведет к региональной военно-политической интеграции. Поводом для атаки на государство может послужить тот факт, что оно принадлежит к другому военному блоку, политико-экономическому союзу вследствие политического или дипломатического конфликта и т.д. Тенденция созидания блоков и военно-политических союзов, нахождение государства в сфере влияния военного или политико-экономического союзов представляет естественную политико-экономическую закономерность.

В повседневной жизни информация стала занимать лидирующее место на фоне стремительного развития компьютерных технологий, которые заняли превалирующую позицию в виртуальном и реальном пространстве. Количество интернет-пользователей растет в геометрической прогрессии, а все это связано с различными внешними и внутренними политическими ситуациями, касающимися каждого государства.

Для XXI века характерен избыток информации, которая очень часто является ложной. Каждый человек имеет возможность стать создателем какой-либо информации, не содержащей истины и распространить ее. В современном законодательстве предусмотрена ответственность за распространение ложной информации в обществе, так как следствием этого является факт массовых выступлений, демонстраций, митингов, пикетирований и протестов.

Преступность в сети Интернет набирает свои обороты ежедневно, что очень сильно отрицательно воздействует на обычных пользователей. Каждый человек не всегда задумывается над тем, что лично он может стать жертвой преступника и снижает свою бдительность, хотя повсеместно мы замечаем ин-

формационные материалы о предупреждении преступности в сети, чтобы обезопасить себя от нежелательных посягательств.

Для предотвращения и противодействия преступности в сети Интернет идет разработка новых программных средств для реализации борьбы с киберперступностью в информационном мире. Многие программы, созданные за последние пять лет, уже стали малоэффективными в сфере противодействия киберугрозам. Данный фактор говорит о том, что преступное сообщество не стоит на месте, а также развивается и модернизирует себя.

В современном мире, в силу технологического и информационного прогресса, прослеживается повышенная активность к обмену данными, происходящему в окружающем нас мире. Интернет является очень хорошим средством для обучения, развития себя как профессионала в компьютерной сфере, но этому всячески противостоят киберпреступники, разрабатывающие новые методы уловок. Развитие компьютеризации неизбежно в постиндустриальном обществе. Людям необходимо движение вперед, а это возможно лишь с помощью новых технологий.

Обеспечение национальной безопасности России будет реализовано, в первую очередь, в связи с противодействием киберпреступности, которая является в современном мире одной из основных глобальных проблем международного масштаба.

В настоящее время противодействие киберугрозам осуществляется всевозможными методами, потому что они могут угрожать безопасности государства, вместе с чем могут пострадать все граждане. Нередко случается, что преступные деяния совершаются группой лиц, которые преследуют экономическую выгоду посредством причинения вреда другим людям.

С целью засекречивания своей личности преступники часто используют средства общего пользования, чтобы их было тяжело вычислить, а также программы, которые скрывают IP-адрес своего компьютера, что делает вычисление невозможным.

Для противодействия данным преступлениям создано специализированное Управление «К» под управлением МВД России. Данное структурное подразделение осуществляет борьбу с преступлениями в сфере информационных технологий, а также с незаконным оборотом радиоэлектронных средств и специальных технических средств.

Указанная организация относится к одним из самых засекреченных подразделений МВД России. В данной структуре используются засекреченные программные и математические обеспечения, которые эффективно противодействуют киберпреступности, создавая мощную систему безопасности.

Помимо этого, важно выделить фактор информирования граждан о возможных информационно-преступных посягательствах. В настоящее время с киберпреступностью ведется борьба на международном уровне, так как преступники представляют угрозу для каждого государства, угрожая взломом государственных систем. Именно с целью обеспечения безопасности и суверенности государства и граждан необходимо разрабатывать определенные про-

граммы, в том числе и антивирусные, которые будут блокировать возможные попытки взлома операционных систем.

В первую очередь, они необходимы для оснащения специализированных подразделений по информационной безопасности, которые будут осуществлять мониторинг и фиксировать базу злоумышленников, с последующим вычислением и привлечением к ответственности за совершенные преступления против личности, общества и государства в целом.

Таким образом, можно сделать вывод, что для борьбы с киберпреступностью необходимы специализированные лицензионные программные средства, которые будут осуществлять защиту общества и государства от киберпреступлений.

3.5. Мероприятия по противодействию мошенническим действиям в сфере информационных технологий

Нынешняя информационная среда стала основным элементом складывающихся общественных отношений. Как правило, все социальные процессы и отношения между ними носят как позитивный, так и негативный характер. Все явления, которые происходили ранее при непосредственном контакте между людьми, заменились процессами в информационной сети.

Современный информационный мир обретает дистанционный режим «работы», даже особо тяжкие преступления без серьезных усилий можно совершить, используя новые разработки преступного характера.

Стремительный рост преступных деяний, реализуемых посредством информационных технологий, выпал на 2020 год. Практически все сферы общественной деятельности перешли в онлайн-среду: обучение в школах, университетах, работа магазинов – все это стало причинно-следственной связью со сложной эпидемиологической обстановкой во всем мире, связанной с ограничениями COVID-19.

Пользовательский состав в сети Интернет возрос по причине массового закрытия предприятий и офисов и введения карантина на неопределенный срок или вовсе потери людьми своих рабочих мест и вакансий.

Возросли преступные деяния в сфере мошенничества, совершаемые с использованием информационно технологий или в сфере компьютерной информации. Количество зарегистрированных мошенничеств с использованием информационных технологий составляет 210 493 за отчетный период с января по декабрь 2020 года, из которых раскрыто всего 13 255 преступлений [84].

Раскрыть и пресечь факт совершенного мошенничества в сфере IT-технологий очень непросто по разным причинам. Множество факторов влияет на результативное совершение мошеннических действий в отношении законопослушного гражданина:

1. Отсутствие знаний у граждан о возможных мошеннических посягательствах в сети Интернет.

2. Непрерывное развитие преступной среды и появление новых способов преступного посягательства.

3. Психологическая обработка жертвы на основе доверия.

4. Умение преступников манипулировать психологическим сознанием человека.

5. Создание неожиданных ситуаций для жертвы с целью запугивания и принятия необдуманных действий.

С развитием онлайн-банков, увеличением количества в них пользователей, банковским организациям приходится реорганизовывать и в корне менять систему безопасности для защиты потребителей.

Методом противодействия преступлениям и главной задачей стало усиление системы безопасности, введение новых технологий по обеспечению информационной безопасности, анонимности баз данных, серверов, подключение наилучших антивирусных программ – все это с целью противодействия мошенническим посягательствам и защиты персональных данных граждан.

Сотрудникам банка необходимо проверять достоверность поступающих сведений. Немаловажным является обеспечение защиты, после прохождения которой лицо сможет получить кредитные денежные средства на свой счет, так как нередко случается, что перевод денежных средств направляется на неизвестный счет злоумышленника с оформлением на потерпевшего гражданина.

Для борьбы с мошенничеством в сети Интернет необходимым является разработка нового программного обеспечения, которое будет организовывать безопасное пользование. Для того, чтобы снизить уровень мошенничества, необходим усиленный контроль за теми методами, с помощью которых реализуются преступные деяния. К примеру, необходимо запретить продажу «безымянных» sim-карт, которые позволяют стать полностью анонимным и незарегистрированным в базе, что усложняет поиск преступника.

Сложной для решения проблемой остается контроль за деятельностью магазинов, организующих прокажу sim-карт без паспортной регистрации. За совершение данных манипуляций необходимо ввести ответственность, чтобы минимизировать подобные случаи. Другим фактором является массовое информирование граждан, чтобы обеспечить теоретическую базу о всевозможных вариантах посягательств, которые трудно предугадать и предотвратить.

Таким образом, можно сделать вывод, что в современном мире уровень мошенничества достигает максимума. С ним ведут борьбу специализированные структуры МВД, ФСБ, ОЭБиПК с целью минимизации уровня преступности в данной сфере. В первую очередь необходимо массовое информирование граждан о существующей угрозе. Во-вторых, способом противодействия мошенническим преступлениям являются специальные программы для телефонов и программные средства для компьютеров.

Очень хорошо зарекомендовали себя программы, распознающие местоположение звонка и его рейтинг, который отображается в стандартном или мошенническом списках, тем самым обеспечивая автоматическое предупреждение граждан, обеспечивает охрану персональных данных, денежных средств, паролей и иной приватной информации.

Вопросы для самоконтроля:

1. Чем объясняется проблема анонимизации личности правонарушителя?
2. Что может облегчить раскрытие личности преступника в виртуальном пространстве?
3. В чем заключается особенность следов, оставляемых преступником при совершении преступления с использованием ИКТ?
4. Какие действия должны предпринимать граждане с целью обезопасить себя от противоправных информационных воздействий?
5. В чем заключается профилактика информационных преступлений?
6. Что можете сказать о преступлениях, совершенных с помощью сети Интернет? В чем заключаются их особенности?
7. Какие мероприятия проводятся по реализации противодействия преступлениям, совершаемым в сети Интернет со стороны МВД России?
8. Какова динамика преступлений, совершаемых в сети Интернет?
9. Какой вид преступлений, совершаемых в сети Интернет, является самым распространенным?
10. Что представляет собой кардинг?
11. Что представляет собой фишинг?
12. В чем заключается метод клонирования?
13. Каким образом можно организовать противодействие преступлениям, совершаемым в сети Интернет, с использованием системы безопасности технических устройств?
14. В чем заключаются уязвимости бесконтактной оплаты NFS?
15. Каковы способы защиты граждан от злоумышленников в виртуальном пространстве?
16. Какие средства смогут эффективным способом противодействовать взлому персональной системы граждан?
17. В чем заключается главная задача МВД России в условиях формирования информационного общества?
18. В чем заключается противодействие информационной преступности в социальных сетях?
19. В чем в настоящее время заключается задача специалистов в области информационной безопасности?
20. Каким образом осуществляется противодействие наркотрафику в сети Интернет?
21. Что входит в состав мероприятий по противодействию киберпреступности?

ГЛАВА 4.
ОСНОВНЫЕ ПОНЯТИЯ И КЛАССИФИКАЦИЯ СИСТЕМНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

4.1. Основные понятия, назначение и классификация программного обеспечения

Рассматривая любую компьютерную систему как симбиоз аппаратных средств и программного обеспечения, особое внимание следует обратить на вторую компоненту. Причин этому несколько: начиная от сложности разработки и заканчивая стоимостью приобретения лицензий на использование программного обеспечения.

Но главным фактором является то, что в основу функционирования компьютера положен ***программный принцип управления***, т.е. компьютер выполняет только операции, находящиеся в оперативной памяти, которые записаны в виде команд в программах. Поэтому ключевым элементом программного обеспечения компьютера является системное программное обеспечение. Это самая сложная и, соответственно, самая дорогая составляющая программного обеспечения.

Системные программы служат интерфейсом между аппаратными ресурсами компьютера и пользователем – человеком или периферийным устройством. В общем случае под ***интерфейсом*** понимаются средства взаимодействия, средства связи, сопряжения, согласования между пользователем (человеком) и компьютерной системой.

Всего различают три вида ***интерфейса***:

1. ***Физический*** интерфейс – взаимосвязь на уровне электронных компонент.
2. Интерфейс ***программиста*** – комплекс правил и соглашений о стыковке программ.
3. Интерфейс ***пользователя*** – набор средств диалога, взаимодействия программы (компьютера) с человеком. Такой диалог обеспечивается через основные элементы интерфейса: меню и окно.

Схема современного интерфейса пользователя с аппаратно-программной средой компьютера представлена на рисунке 4.

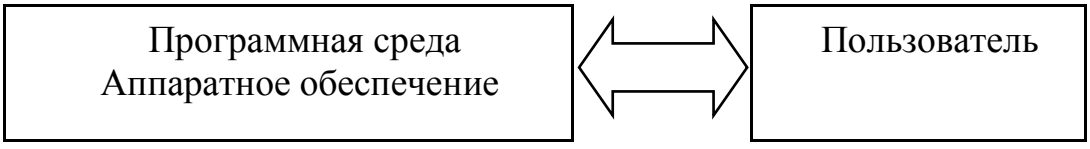

Рисунок 4. Интерфейс пользователя с аппаратно-программной средой компьютера

Программное обеспечение ЭВМ является оболочкой ее аппаратной среды и обеспечивает интерфейс с пользователем.

Программное обеспечение (ПО) – составляющая информационных технологий, включающая компьютерные программы и данные, предназначенные для решения определенного круга задач и хранящиеся на машинных носителях.

Программное обеспечение представляет собой либо данные для использования в других программах, либо алгоритм, реализованный в виде последовательности инструкций для процессора.

Все программное обеспечение для компьютеров может быть представлено тремя видами программ: системным программным обеспечением, средствами для создания приложений, а также прикладным программным обеспечением. Классификация ПО представлена на рисунке 5.

Прикладное программное обеспечение – программы, предназначенные для выполнения определенных пользовательских задач и рассчитанные на непосредственное взаимодействие с пользователем.

Инструментальное программное обеспечение – программное обеспечение, предназначенное для использования в ходе проектирования, разработки и сопровождения программ. В ходе изучения данного курса вы не будете изучать инструментальное программное обеспечение, которым пользуются только специалисты в области информационных технологий.

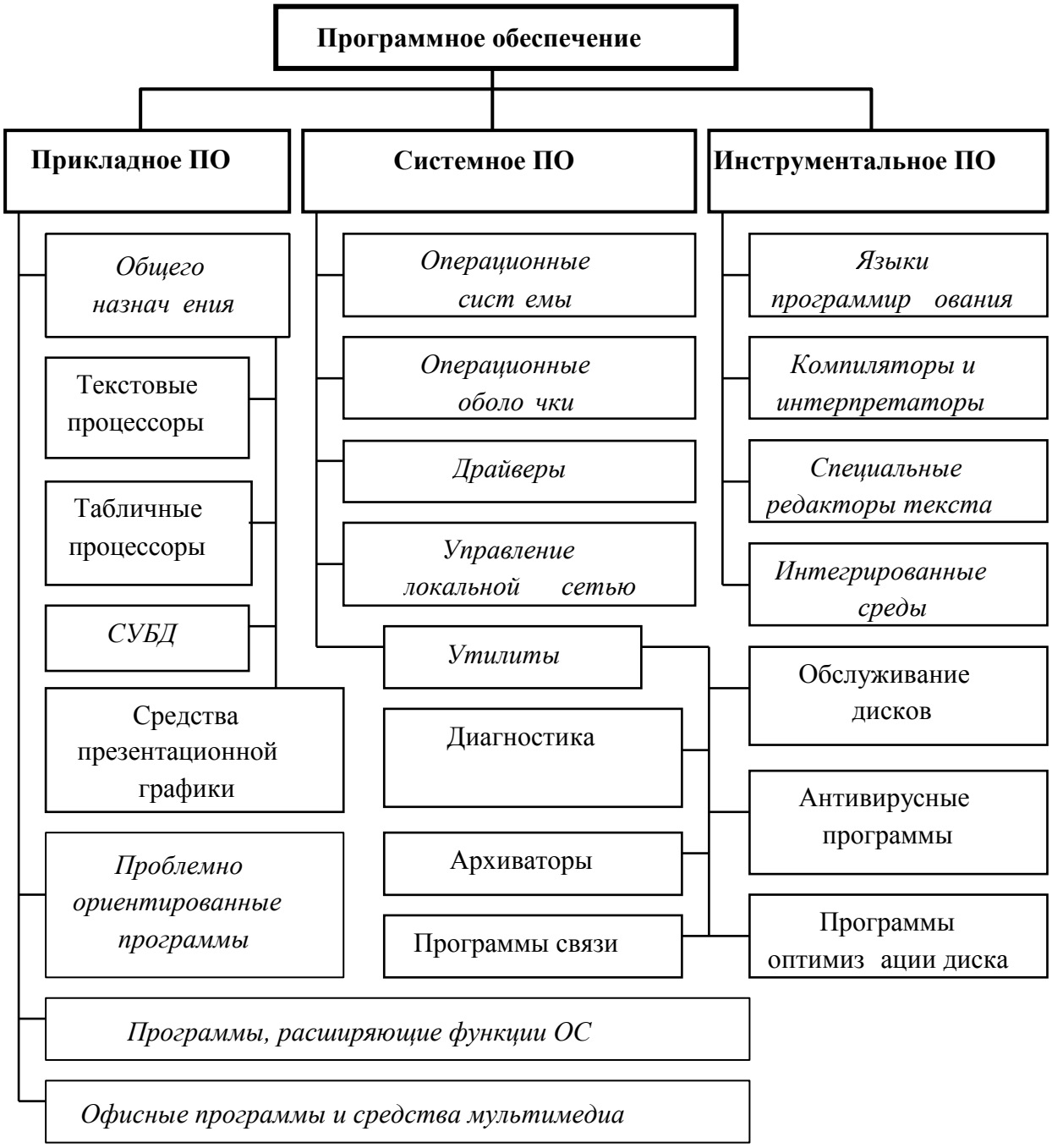

Рисунок 5. Классификация программного обеспечения

Системное программное обеспечение – это набор программ, которые управляют компонентами вычислительной системы, такими как процессор, коммуникационные и периферийные устройства, а также которые предназначены для обеспечения функционирования и работоспособности всей системы. В отличие от прикладного, системное программное обеспечение (операционная система) используется для обеспечения работы компьютера самого по себе и выполнения прикладных программ.

В соответствии с ГОСТ 19781-90 ЕСПД «Обеспечение систем обработки информации программное» ***программное обеспечение*** – совокупность программ системы обработки» информации и программных документов, необходимых для эксплуатации этих программ.

В соответствии с ГОСТ Р ИСО/МЭК 9126-93 «Оценка программной продукции. Характеристики качества и руководства по их применению» ***программное обеспечение (software)*** – программы, процедуры, правила и любая соответствующая документация, относящиеся к работе вычислительной системы.

Программная продукция (software product) – программный объект, предназначенный для поставки пользователю.

Для работы на современных персональных компьютерах с системными или прикладными программами не требуется специальных навыков программиста и знаний языков программирования. Программное обеспечение (ПО) персональных компьютеров (ПК) можно разделить на:

– ***системное*** – обеспечивает автоматическую загрузку и функционирование ПК, а также общее управление компьютером и профилактическое обслуживание;

– ***прикладное*** – обеспечивает решение пользовательских задач.

Для задач программирования – т.е. разработки системных и прикладных компьютерных программ существует отдельный вид ПО – ***инструментальное ПО***.

В связи с повсеместным использованием технологий графических интерфейсов (visual-технологии) и объектного программирования граница между прикладным и инструментальным программным обеспечением практически стерта. Например, к какому виду ПО можно отнести пакет MSOffice 2010, в который, помимо общеизвестных прикладных возможностей, включены средства поддержки языка программирования VBA (Visual Basic for Applications) или создания WEB-страниц на языке HTML или пакет 3-мерного графического моделирования Autodesk 3d Studio Max.

Программное обеспечение является объектом авторского права и охраняется законодательством Российской Федерации как литературные произведения (Гражданский кодекс РФ от 18.12.2006 № 230-ФЗ, часть 4).

Ниже приведены некоторые ***типы лицензий*** на программное обеспечение:

Freeware – бесплатная программа без функциональных ограничений. Сфера использования регулируется авторским правом. Владелец программы может запретить ее свободное распространение или коммерческое использование. Например, программа может быть бесплатна только для дома или для учебного процесса при условии некоммерческого использования.

Shareware – условно-бесплатная программа. Коммерческая программа с бесплатным периодом использования и (или) ограниченным функционированием. Предлагается сначала опробовать программу в действии, а затем оплатить ее полную стоимость. «Условность» может лежать в очень широких границах, от периодического напоминания о необходимости заплатить за программу при каждом запуске до блокирования основных функций, ограничивающих использование программы по прямому предназначению.

Trial, trial ware – пробная (оценочная) версия программы. Ограничена временем использования или блокированием отдельных функций.

***Demo,* demo ware** – ограниченная версия программы, демонстрирующая ее основные возможности.

Adware – бесплатная рекламно-ориентированная программа без функциональных ограничений, но со встроенными окнами для показа рекламы, которая может подгружаться через Интернет. Модуль фоновой загрузки рекламы без уведомления пользователя фактически является «трояном».

Donate ware – программа, не требующая обязательной регистрации и оплаты для нормального функционирования, но ненавязчиво предлагающая оказать какую-либо услугу автору, в том числе и денежное пожертвование.

Open source – бесплатное программное обеспечение с «открытым» исходным кодом, т.е. возможностью его модифицировать без согласования с автором. Используется «как есть» (as is) без каких-либо авторских гарантий.

Beta – некоммерческая версия программы для тестирования ее возможностей, как правило, ограниченным кругом пользователей. В процессе создания программа проходит несколько этапов, характеризующихся ее готовностью к окончательному выпуску: Alpha, Beta, RC (Release Candidate).

На стыке программного и аппаратного обеспечения есть еще ***firmware (программируемое оборудование*)** – управляющая программа для однократной записи в энергонезависимую память оборудования («прошивки»). Пользователь получает систему с установленным на заводе Firmware и не задумывается о нем (хотя многие устройства допускают обновление «прошивок» новыми версиями). Например, BIOS на материнской плате ПК или операционная система на сотовых телефонах.

В соответствии с ГОСТом 19781-90 ***прикладная программа*** – программа, предназначенная для решения задачи или класса задач в определенной области применения системы обработки информации. Совокупность прикладных программ, предназначенная для решения задач определенного класса, называется ***пакетом прикладных программ*.**

Прикладные программы можно классифицировать, например, ***по типу*:**

– ***общего назначения*** (текстовые, графические, аудио-, видеоредакторы, аудио-, видеоплейеры, системы управления базами данных, электронные таблицы, веб-браузеры и т.п.);

– ***профессионально ориентированные*** (экспертные системы, системы автоматизированного проектирования, обеспечение АРМ, АСУ, АСУ ТП, геоинформационные системы);

– ***культурно-развивающие*** (мультимедиа энциклопедии, справочники, игры и т.п.);

– ***контрольно-обучающие*** (электронные курсы, тесты, симуляторы и т.п.).

В органах внутренних дел прикладное программное обеспечение входит в состав автоматизированных рабочих мест или автоматизированных информационных систем по направлениям профессиональной деятельности. Функционирование таких систем обеспечивается специализированным системным ПО.

4.2. Системное программное обеспечение и операционные системы

После загрузки операционной системы пользователь и другие программы получают возможность управления компьютером, т.е. возможность непосредственно решать прикладные задачи: производить вычисления, готовить документы и выводить на печать, моделировать различные процессы, играть в игры и т.д. – т.е. использовать компьютер по его прямому предназначению – как средство автоматизации человеческой деятельности.

Системная программа – программа, предназначенная для поддержания работоспособности системы обработки информации или повышения эффективности ее использования в процессе выполнения прикладных программ.

Управляющая программа – системная программа, реализующая набор функций управления, в который включают управление ресурсами и взаимодействием с внешней средой системы обработки информации, восстановление работы системы после проявления неисправностей в технических средствах.

Супервизор (ядро) – часть управляющей программы, координирующая распределение ресурсов системы обработки информации.

Программа обслуживания – программа, предназначенная для оказания услуг общего характера пользователям и обслуживающему персоналу системы обработки информации.

В настоящее время терминология естественно изменилась, но типовой состав системного ПО компьютеров с архитектурой IBM PC остался практически тем же.

BIOS – базовая система ввода-вывода размещается в специальной микросхеме на системной плате и устанавливается на заводе-изготовителе (firmware), но может быть «перепрошита» с учетом модификации исходных кодов.

На место BIOS приходит UEFI – программируемый интерфейс между операционной системой и низкоуровневыми микропрограммами (прошивками) аппаратных устройств ПК. UEFI инициализирует оборудование при включении ПК и передает управление загрузчику операционной системы. В отличие BIOS, который всегда жестко прошит в соответствующем чипе на системной плате, коды UEFI находятся в специальной директории (EFI), которая физически может располагаться и в микросхеме памяти на системной плате, и в разделе на жестком диске компьютера, и во внешнем сетевом хранилище.

Операционная система – совокупность системных программ, предназначенная для обеспечения определенного уровня эффективности системы обработки информации за счет автоматизированного управления ее работой и предоставляемого пользователю определенного набора услуг (ГОСТ 15971-90 «Системы обработки информации. Термины и определения»).

Основные ***функции*** современных **ОС** ПК:

– управление интерфейсами передачи данных между системными и периферийными устройствами;

– управление оперативной памятью (загрузка программ, распределение между процессами, очистка, поддержка файла подкачки – виртуальной памяти);

– обработка запросов обслуживания внешних устройств и программ (ввод и вывод данных, запуск и остановка библиотечных процедур и функций);

– поддержка файловых систем хранения данных на внешних носителях;

– обеспечение интерфейса пользователь-компьютер;

– профилактика, диагностика и восстановление работоспособности компьютера после сбоев;

– защита процессов и данных от несанкционированного доступа или воздействия;

– поддержка многозадачного и многопользовательского режима работы ПК с разграничением доступа к его ресурсам.

Интерфейс – совокупность средств и правил, обеспечивающих взаимодействие устройств вычислительной машины или системы обработки информации и (или) программ.

Основные компоненты операционной системы:

1. ***Загрузчик*** – небольшая программа для передачи управления от BIOS к ОС, размещаемая на внешнем устройстве по определенному адресу и обеспечивающая загрузку ядра операционной системы.

2. ***Ядро ОС (супервизор*)** – основная часть операционной системы, управляющая аппаратными ресурсами вычислительной системы (процессор, память и устройства ввода-вывода) и предоставляющая программным процессам координированный доступ к этим ресурсам. На уровне ядра могут быть реализованы поддержка файловой системы и управление обменом по локальной вычислительной сети.

3. ***Драйвер устройства*** – программа, предназначенная для управления периферийным устройством, в том числе файловой системой для устройств внешней памяти. С одной стороны, драйвер поддерживает интерфейс конкретного устройства, с другой – конкретной операционной системы.

Другими словами, операционная система управляет некоторым «виртуальным» устройством, которое понимает ее стандартный набор команд. Драйвер переводит эти команды в команды, которые понимает физическое устройство. Наличие драйверов позволяет разработчикам нового компьютерного оборудования «подружить» его с любой операционной системой.

4. ***Средства поддержки файловых систем*** **(ФС)** – правила и методы организации, хранения и именования данных, размещаемых на внешних носителях. ОС и ФС взаимодействуют через драйверы файловой системы.

5. ***Командный процессор (интерпретатор системных команд*)** – компонент операционной системы, отвечающий за выполнение отдельных системных инструкций, вводимых пользователем в специальной командной строке в текстовом формате. При необходимости выполнить заданную последовательность инструкций они могут быть сгруппированы в командный файл.

6. **Операционная оболочка** – программное средство автоматизированного управления компьютером с интуитивно понятным пользовательским интерфейсом (как правило, графическим с поддержкой манипулятора «мышь»). Служит альтернативой командному процессору для ввода и выполнения сис-

темных инструкций, в том числе файловых операций. Может входить в состав дистрибутива ОС (проводник MS Windows, рабочий стол, панель управления), а может существовать как отдельная программа независимого разработчика (Total Commander).

С 1990-х годов наиболее распространенными операционными системами персональных компьютеров являются ОС семейства Windows и семейства UNIX (Linux и Mac OS X).

Служебные и сервисные программы – совокупность программ, автоматизирующих процессы установки и настройки различных параметров системы, пользовательского интерфейса, диагностики, профилактики, оптимизации и поддержки системы в актуальном работоспособном состоянии, восстановления после сбоев и т.д.

В большинстве случаев все необходимые функции по обслуживанию компьютера можно реализовать встроенными средствами операционной системы. В MS Windows к таким средствам можно отнести Центр обновления, Центр поддержки, Брандмауэр, Диспетчер учетных данных, Архивацию и восстановление системы и др.

Особое место занимают ***средства обеспечения информационной безопасности*** – системные программы обеспечения конфиденциальности, целостности и доступности обрабатываемых на компьютере данных с учетом правил разграничения доступа.

В качестве примера можно привести программу архивации данных True Image, которая позволяет создавать резервные копии операционной системы, приложений, пользовательских настроек и всех имеющихся данных, а также надежно уничтожать всю конфиденциальную информацию, ставшую ненужной. С ее помощью можно выполнять резервное копирование файлов и папок, настроек и писем почтовых клиентов Майкрософт и даже целых дисков и их разделов. Acronis Online Backup позволяет хранить самые важные файлы в удаленном хранилище. Данные будут защищены даже в случае потери, кражи или уничтожения компьютера. Непрерывная защита Acronis периодически (каждые пять минут) сохраняет изменения, произошедшие в системе и файлах, что, при необходимости, дает возможность легко вернуться к состоянию на любой момент времени. Все это позволяет легко и быстро восстановить данные из резервных копий в случае отказа жесткого диска, вирусной атаки или атаки вредоносного программного обеспечения.

Широкое применение у пользователей имеют программы поддержки оптических дисков (создание образов, запись, диагностика), например, от производителей Nero или Ashampoo.

Ни один компьютер в современной организации не функционирует без защиты от вредоносных программ. В дополнение к функциям классической антивирусной защиты (сигнатурный поиск в системе известного вредоносного ПО) антивирусные программные продукты применяют проактивные технологии (поиск уязвимостей и предотвращение заражения системы), а также средства защиты от сетевых атак. Лидерами антивирусной индустрии в нашей стране являются «Лаборатория Касперского» и компания «Доктор Веб».

Не помешают на компьютере специализированные программы для тонкой настройки параметров ОС – твикеры (tweaker), которые используют стандартные возможности системы (например, настройки реестра) или скрытые от обычного пользователя.

Динамические библиотеки – файлы, содержащие исполняемые коды и данные, которые могут использовать несколько программ одновременно.

В операционных системах семейства MS Windows большая часть функциональных возможностей операционной системы обеспечивается динамическими библиотеками (.DLL, .OCX., .CPL).

Когда несколько программ используют одну и туже библиотеку функций (например, вывод на печать), размер программ на диске и в оперативной памяти может значительно уменьшится, скорость загрузки, и, соответственно, производительность увеличится. Наиболее востребованные библиотеки могут размещаться в оперативной памяти сразу после запуска компьютера и выполняться в фоновом режиме (во время «простоя» центрального процессора).

Итак, системное программное обеспечение, в отличие от прикладного, не решает конкретные пользовательские задачи, а обеспечивает работу компьютера и других программ, управляет информационными ресурсами вычислительной системы, защищает информацию и т.д.

В соответствии с принципами фон Неймана компьютеры могут выполнять только инструкции, находящиеся в оперативной памяти, – достаточно дорогостоящем устройстве относительно небольшой емкости. Вместе с тем основная часть программного обеспечения размещается на устройствах внешней памяти (магнитных или оптических дисках, флэш-памяти и т.д.) в файлах и папках (каталогах).

Файл – поименованная область на устройстве внешней памяти, организованная для долговременного хранения однородных данных.

Пользователь или программа с файлами могут выполнять ***файловые операции*:** создание, копирование, удаление, загрузка в память и выполнение, извлечение данных и т.д., в зависимости от типа файла.

Папка (каталог) – поименованная область на устройстве внешней памяти, организованная для группирования файлов по каким-либо признакам.

Каталоги могут образовывать иерархические структуры из нескольких отдельных деревьев (как в DOS/Windows) или же объединяться в одно дерево, общее для всех дисков (как в NIX-системах). Каталог верхнего уровня называется ***корневой***.

Файловая система – это совокупность правил и способов организации данных на физическом пространстве носителя, а также их идентификационные признаки для обработки на компьютере.

Идентификатором файла являются его имя и адрес на внешнем носителе. Синтаксис идентификационной записи зависит от конкретной операционной системы.

Например, в MS Windows запись:

c:\win\system32\diskcopy.com

идентифицирует файл с именем «*diskcopy»*, расширением «*com*» на диске «*c»* в папке «*system32»,* вложенной в папку *« win».*

Символ «:» – указывает на имя тома, «\» – разделяет имена папок и файлов, «.» – отделяет имя файла от его расширения.

Том – область памяти на жестком диске. Том форматируется для определенной файловой системы, такой как FAT или NTFS, и обозначается буквой. Содержимое тома можно просмотреть, щелкнув его значок в проводнике Windows или в окне «Мой компьютер». Один жесткий диск может содержать несколько томов; тома также могут занимать несколько дисков.

Раздел диска – часть физического диска, которая ведет себя как отдельное устройство. Для хранения данных на созданном разделе необходимо сначала отформатировать его и назначить букву диска.

Разделы на базовых дисках называют ***базовыми томами***; к ним относятся основные разделы и логические диски. Разделы на динамических дисках называют динамическими; к ним относятся простые, чередующиеся, составные, зеркальные тома и тома RAID-5.

Если файл размещен в компьютерной сети, то его ***адрес*** может выглядеть так:

http://www.opennet.ru/docs/RUS/tcp_conf/tcp01.html,

где «http:» – протокол обмена, а «www.opennet.ru» – доменное имя ресурса в сети Интернет.

В принципе, файловая система не должна зависеть от ОС, но любая ОС через драйвера и интерфейс программирования приложений (API) поддерживает определенные файловые системы.

Расширение имени файла указывает на его тип.

По типу носителя файловые системы можно классифицировать следующим образом:

– с произвольным доступом (например, жесткий диск): FAT32, NTFS, ext2 и др.;

– с последовательным доступом (например, магнитные ленты): QIC и др.;

– для оптических носителей: ISO9660, HFS, UDF и др.;

– для флэш-памяти: YAFFS, Extreme FFS, exFAT;

– сетевые файловые системы: NFS, CIFS, SSHFS, GmailFS и др.

Таким образом, основные ***задачи файловой системы***:

– отображение логической модели файловой системы на физическую организацию хранилища данных;

– идентификация имен файлов, размещенных на внешних носителях;

– поддержка интерфейса файловых операций;

– обеспечение надежности хранения файлов, устойчивости к сбоям питания, ошибкам аппаратных и программных средств;

– обеспечение механизма разграничения доступа пользователей и программ при совместной работе с файлами.

В функции современных операционных систем входит обеспечение выполнения файловых операций как для программ, так и в автоматизированном режиме под управлением пользователя.

Пользователь может манипулировать файлами с помощью командного процессора (интерпретатора командной строки) или графической оболочки (проводник Windows).

В случае если необходимо выполнить групповую операцию с несколькими файлами, их можно описать с помощью символов маски: «*» и «?».

Символ «*» маскирует в своей позиции любое число любых символов. Символ «?» маскирует в своей позиции один символ, что представлено на рисунке 6.

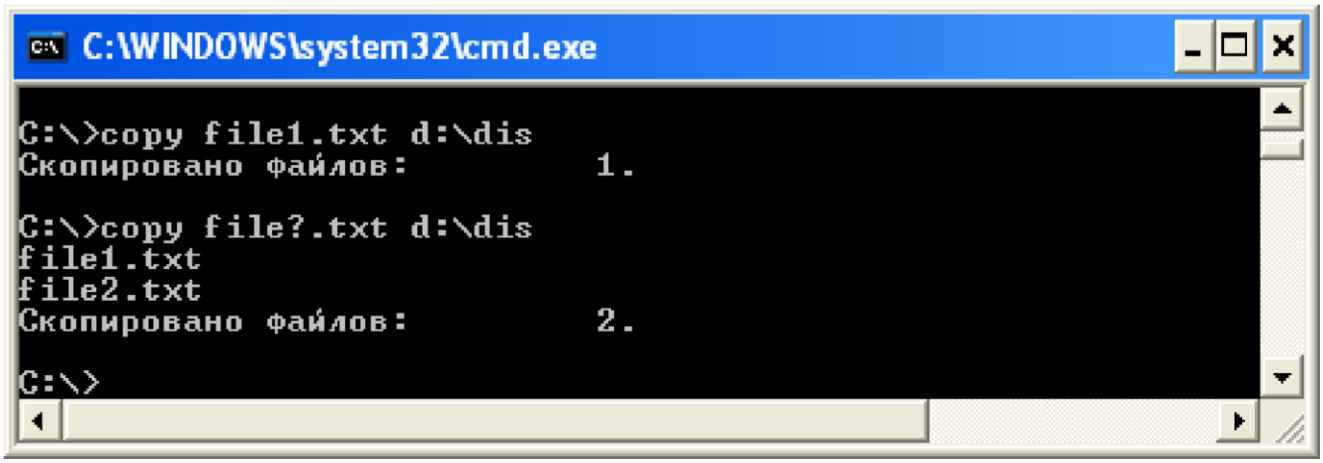

Рисунок 6. Пример применения маскирующего символа «?»

Вопросы для самоконтроля:

1. Что является основной компонентой в компьютерной системе и почему?
2. В чем заключается программный принцип управления?
3. Для чего служат системные программы?
4. Какие виды пользовательских интерфейсов различают?
5. Что представляет собой программное обеспечение?
6. В чем заключается назначение прикладного ПО?
7. В чем заключается назначение инструментального ПО?
8. В чем заключается назначение системного ПО?
9. Что представляет собой технология графического интерфейса?
10. В чем заключается особенность freeware?
11. В чем заключается особенность shareware?
12. В чем заключается особенность trialware?
13. В чем заключается особенность adware?
14. В чем заключается особенность donateware?
15. На какие группы делятся прикладные программы по их типу?
16. Что такое системная программа?
17. Что такое управляющая программа?
18. В чем заключается назначение BIOS?
19. Какие основные функции выполняет ОС ПК?
20. Каковы основные компоненты операционной системы?
21. Для чего предназначены служебные и сервисные программы?
22. Что представляют собой программные средства обеспечения информационной безопасности?
23. Что представляет собой программа True Image?
24. В чем состоит защита от вредоносных программ?
25. Что представляют собой динамические библиотеки?
26. Что такое файл?
27. Как организована файловая система?
28. Что такое том?
29. На что указывает расширение файла?
30. Как можно классифицировать файловые системы?

ГЛАВА 5.
СИСТЕМНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ, ИСПОЛЬЗУЕМОЕ ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

5.1. Анализ состава и объема рынка программного обеспечения в области противодействии преступлениям в сфере информационной безопасности

Научный и практический интерес к проблематике киберпреступности возрастает с каждым годом по мере развития и усложнения программного обеспечения и компьютерных систем. Во всех развитых странах происходит повсеместная цифровизация всех учреждений, предприятий, социальной инфраструктуры и, соответственно, повышается количество различных компьютерных устройств со сложной архитектурой и немалым количеством уязвимостей.

Всемирное киберпространство также не является полностью защищенным. В Интернет за 2019 год утекло почти 14 миллиардов записей, содержащих конфиденциальную информацию. Скачок общего количества случаев несанкционированного доступа к информации в России составил более 40%, а во всем мире он составлял лишь 10%. В то же время на мировом уровне этот показатель составляет только 20% по сравнению с предыдущим периодом. Сегодняшние способы совершения атак становятся все более изощренными. Согласно статистике, более половины мошеннических схем реализуются во всемирной сети Интернет и около трети – с помощью мобильной связи [10, с. 46]. Каждый десятый мошенник использует банковские карты для совершения мошенничества. В среднем, около 80% пострадавших от действий киберпреступников несут небольшой ущерб – менее 5 тыс. рублей. Обычно один из пяти потерпевших не сообщает о произошедшем в полицию. Однако их количество по оценкам специалистов, может достигать 200–300 млн в год.

Информация – важнейший ресурс в жизни каждого человека, ее можно даже назвать валютой. В соответствии с этим информация и цифровые данные подвергаются высокому риску применения к ним все большего количества угроз с целью несанкционированного проникновения в систему или получения информации. Ведь тот, кто владеет информацией, – тот владеет миром. Борьба за информацию происходит не только между хакерскими группировками и компаниями, но и между правительствами различных стран с целью политического, военного превосходства в мире. С каждым годом DDoS-атаки, перехват сетевых данных, заражение вирусным ПО и другие киберпреступления становятся более изощренными, продуманными и набирают обороты.

В основном, 90% всех атак составляют простые вирусы – черви, трояны, фишинговые письма, вредоносный код, встроенный в пользовательские файлы и программы [83]. В основном такие вирусы не нацелены на конкретный компьютер и их главной задачей является максимальное распространение и установка на большом количестве компьютеров. Для подобных задач хакеры нани-

мают специальных людей, задача которых – распространить вирус на большое число систем. Также существуют целевые атаки, которые составляют 9,9% от общего числа атак. Обычно они направлены на конкретного человека, компьютер или ресурс с целью собрать или украсть данные, деньги со счетов, найти конфиденциальные документы с целью их дальнейшего использования.

Есть даже вирусы, которые собраны специально для определенных компьютеров, нужных злоумышленникам. Такой вирус может попасть на компьютер обычного пользователя, но не сработает, так как «цель не совпала» и будет дальше распространяться с этого и других компьютеров, пока не найдет цель. Причем такой вирус может бродить месяцами по сети, и когда, например, жертва подключится к бесплатному Wi-Fi в кафе, то вирус, находящийся в данной сети, установится на его компьютер и совершит атаку.

В связи с растущим количеством уязвимостей, расширением баз данных, систем хранения и передачи данных каждой организации предстоит в скором времени озаботиться и обеспечить реализацию систем защиты информации, которые будут надежно защищать корпоративную информационную инфраструктуру. Ответственность за организацию системы защиты информации полностью лежит на руководстве организации. Выбирая систему защиты, необходимо учитывать ряд факторов. Такие как размеры предприятия и его сети, техническое оснащение, навыки персонала в сфере соблюдения режима конфиденциальности на предприятии.

Поэтому задача создания такой системы информационной безопасности предприятий является комплексной. При этом руководство должно оценить уровень предполагаемых рисков, ущерба и разработать модель угроз. Для каждого бизнеса она будет разной. Общее – это то, что для нанесения ущерба компании используются информационные технологии. Проведение аудита для обеспечения информационной безопасности необходимо. По результатам анализа определяется комплекс необходимых организационных и программно-технических мер.

Хакерские атаки с каждым годом становятся все разрушительнее: DDoS-атаки, вирусы-шифровальщики, перехват трафика и данных через незащищенные сети. Если раньше атаки были децентрализованными и хакеры не стремились взломать конкретную цель, а просто распространяли вирусы как можно больше, чтобы сделать из компьютеров ботнеты, украсть пароли, личные данные, переписки и аккаунты, то сейчас хакеры действуют по-крупному и даже один вирус может заразить тысячи компьютеров, но подействует он только на том, который является целью преступников.

Те же вирусы-шифровальщики чуть не вывели из строя всю медицинскую инфраструктуру США, когда вирус WannaCry [68] заразил множество медицинских аппаратов и компьютеров в больницах, которые не были хорошо защищены. Поэтому порой от безопасности сети и всех систем предприятия могут зависеть жизни обычных людей. Если хакеры решат взломать атомную электростанцию, систему подсчета голосов на выборах, политика в социальных сетях – это может стать угрозой мирового масштаба. В ближайшие пару лет

возможна реализация атаки, которая в буквальном смысле сможет вернуть нас в каменный век, если мы не будем готовы к этому.

Вирусы в своей основе используют уязвимости систем, которые являются ошибкой разработчика программного обеспечения, но иногда подобного рода уязвимости делаются предумышленно для использования разработчиком или же для предоставления полного доступа к устройствам специальным службам и правоохранительным органам. Но зачастую происходит так, что преступники находят эти уязвимости и реализуют их в своих атаках. Такие уязвимости называются «критическими» или «уязвимостями нулевого дня». Их особенность заключается в том, что подобные уязвимости невозможно закрыть быстро, и для устранения подобного изъяна может потребоваться переписывать большую часть программного кода, а для любого разработчика это слишком сложно и затратно.

Рассмотрим далее статистические данные по объемам и сегментам рынка ПО для обеспечения информационной безопасности в Российской Федерации в 2020 году.

1. Рынок информационной безопасности.

Общий объем рынка информационной безопасности в Российской Федерации по итогам 2020 года по общей оценке составляет 142,6 млрд рублей (см. табл. 1) [70].

Таблица 1. Объем рынка информационной безопасности в Российской Федерации по сегментам в 2020 году

Сегмент рынка	**Объем (млн руб.)**	**Доля (%)**
Защита компьютерных систем	68 700	48,2
Услуги ИБ	46 500	32,6
Контроль доступа	9 400	6,6
Защита приложений	8 900	6,2
Защита данных	7 600	5,3
Управление ИБ	1 500	1,1
Всего	142 600	100

2. Защита критической инфраструктуры.

Общий объем рынка защиты критической инфраструктуры по итогам 2020 года по общей оценке составляет 68 700 млн рублей (см. табл. 2) [70].

Таблица 2. Объем рынка защиты критической инфраструктуры по сегментам в 2020 году

Сегмент рынка	**Объем (млн руб.)**	**Доля (%)**
Сетевая безопасность	34 700	50,5
Защита конечных точек	22 000	32
SIEM	7 200	10,5
Безопасность промышленных сетей	1 900	2,8
Сервисы киберразведки	700	1
Другое	2 200	3,2
Всего	68 700	100

3. Сетевая безопасность.

Общий объем рынка сетевой безопасности в России по итогам 2020 года по общей оценке составляет 34 700 млн рублей (см. табл. 3) [70].

Таблица 3. Объем рынка сетевой безопасности в России по сегментам в 2020 году

Сегмент рынка	**Объем (млн руб.)**	**Доля (%)**
NGFW / UTM	21 000	60,5
VPN-шлюзы	5 000	14,4
Сетевые системы предотвращения вторжений	3 000	8,6
Сетевые песочницы	1 500	4,3
Безопасные почтовые шлюзы	1 500	4,3
Сетевое детектирование и реагирование	1 000	2,9
Контроль сетевого доступа	900	2,6
Безопасные веб-шлюзы	800	2,3
Всего	34 700	100

4. Услуги по информационной безопасности.

Общий объем рынка категории услуг по безопасности в России по итогам 2020 года по общей оценке составляет 46 500 млн рублей (см. табл. 4) [70].

Как правило, данный сегмент имеет довольно высокие показатели в общем рейтинге. Это обусловлено большим количеством услуг по внедрению средств информационной безопасности, оказываемых преимущественно лидерами рынка. В ближайшем будущем данный сегмент информационной безопасности очень перспективен, поскольку аудит и консультации присутствуют на рынке давно и достигли стабильного состояния, в то же время делегирование обязанностей и полномочий организациям в новинку и к тому же стимулируется внешними экономическими факторами.

Таблица 4. Основные категории услуг по безопасности на российском рынке ИБ в 2020 году

Сегмент рынка	**Объем (млн руб.)**	**Доля (%)**
Внедрение	25 000	53,8
Аутсорсинг	11 000	23,7
Консалтинг	7 000	15,1
Оценка защищенности	800	1,7
Расследования инцидентов	500	1,1
Другое	2 200	4,7
Всего	46 500	100

5. Безопасность приложений.

Общий объем рынка сетевой безопасности приложений по итогам 2020 года по общей оценке составляет 8 900 млн рублей (см. табл. 5) [70].

Программное обеспечение в области информационной безопасности в РФ востребовано не только на рынке РФ, но и на европейских рынках ПО. Российское ПО постоянно развивается, появляются новые решения, модернизируются старые. Современные решения постоянно подстраиваются под конечных пользователей и бизнес в соответствии с их потребностями.

Рынок постоянно масштабируется, так как из-за цифровизации увеличиваются и риски хакерских атак на критическую инфраструктуру с целью кражи данных. Российское программное обеспечение в области информационной безопасности – надежное и современное решение, зачастую обладающее обширными возможностями, гибкостью, постоянно обновляемое и поддерживаемое разработчиками. Вот почему организации в основном выбирают именно его.

Таблица 5. Объем рынка безопасности приложений в России по сегментам в 2020 году

Сегмент рынка	Объем (млн руб.)	Доля (%)
Управление уязвимостями	4500	50,6
Защита от DDoS	1800	20,2
Брандмауэры веб-приложений (WAF)	1500	16,9
Сканеры исходного кода	500	5,6
Другое	600	6,7
Всего	8900	100

5.2. Системное программное обеспечение в области противодействия преступлениям в сфере информационных технологий

Базовый принцип обеспечения корпоративной информационной безопасности в современном мире – принцип «нулевого доверия». Этот принцип заключается в том, что информационная безопасность в компании должна быть тотальной и охватывать не только попытки взлома извне, но и принимать во внимание риск несанкционированных действий изнутри. Подобная система основывается на использовании комбинации из разных программных решений и комплексов ПО [74].

В Российской Федерации существуют контролирующие органы, наблюдающие и обеспечивающие сертификацию и аккредитацию программного обеспечения в области защиты информации. Это соответственно ФСБ России и ФСТЭК России. Аккредитация и сертификация необходима для того, чтобы программное обеспечение соответствовало требованиям и запросам государства и компаний в сфере защиты информации. Также эти органы обеспечивают контроль за тем, чтобы данное программное обеспечение не попадало не в те руки.

Рынок программного обеспечения в области информационной безопасности в Российской Федерации считается одним из самых развитых среди европейских стран [70]. Это напрямую связано с потребностями нашего государства в надежной защите, как собственной инфраструктуры, так и тех организаций, которые работают непосредственно с государством. Даже иностранные компании часто используют именно российские решения, так как они отличаются

своим широким функционалом, высокой степенью защиты и обширным выбором решений.

Рассмотрим комплекс из различных программ для обеспечения информационной безопасности, программ для защиты документооборота, антивирусов для защиты корпоративной информации от злоумышленников и конкурентов.

Системное программное обеспечение защиты информации

SIEM-системы

SIEM (Security Information and Event Management) – комплексные системы агрегации, анализа событий и управления данными об информационной безопасности организации. Это ПО создано для того, чтобы предотвращать утечки данных и закрыть иные бреши в информационной безопасности организации.

IBM QRadar Security Intelligence [61]

IBM QRadar Security Intelligence – платформа, включающая в себя ряд продуктов для обнаружения угроз сетевой безопасности, анализа, оценки и противодействия им. Данное ПО позволяет реализовать и организовать управление событиями, эффективно интегрировать информацию об информационной безопасности в деятельность предприятия. Помогает выявить нештатные ситуации и управлять журналом для решения других задач управления.

Основные возможности:

– единая система анализа угроз, журналов, событий и других маркеров;

– полный анализ информационной инфраструктуры в режиме реального времени;

– обширные возможности анализа сетевого трафика и активности;

– обнаружение и предотвращение инцидентов с высоким приоритетом;

– сбор и обобщение информации о зафиксированных угрозах;

– масштабированный контроль активности в рамках предприятия;

– аудит с помощью технологий искусственного интеллекта и технологий больших данных.

Недостатки:

- для некоторых регистрируемых событий не присваивается категория;
- у некоторых предприятий возникают сложности с запуском такой большой платформы, что в любом случае потребует перестроения процессов на предприятии.

Стоимость:

Доступен 14-дневный пробный период, а также возможность бесплатного использования ПО с ограниченным функционалом. Стоимость лицензии – от 800 долларов в месяц.

Splunk Enterprise Security [67]

Splunk Enterprise Security – инструмент, помогающий в аналитике событий информационной безопасности в организациях. Главной его особенностью является быстрое реагирование на новейшие угрозы и полная совместимость с новыми программно-аппаратными решениями.

Основные возможности:

– мониторинг и анализ угроз в режиме реального времени;

– контроль действий пользователей, программ и сетевых ресурсов в реальном времени;

– обнаружение сложных угроз, в том числе с помощью системы построения взаимосвязей между разными событиями;

– расследование инцидентов информационной безопасности, в том числе установление их масштабов и ущерба.

Недостатки:

– сложность установки корпоративной версии ПО;

– отсутствует русская локализация новых версий ПО.

Стоимость:

Стоимость лицензии начинается от 1800 долларов в год в зависимости от выбранной конфигурации.

McAfee Enterprise Security Manager [65]

McAfee Enterprise Security Manager считается одним из лидирующих программных решений по скорости и полноте обработки информации. McAfee Enterprise Security Manager хорошо подходит для предприятий и организаций, где требуется постоянная обработка и анализ огромных объемов данных.

Основные возможности:

– наличие собранных конфигураций с настроенными сценариями для упрощения безошибочного слияния, что упрощает взаимодействие и обслуживание подобных систем;

– присутствие и постоянное обновление обучающего материала по базовому поведению пользователей;

– мониторинг внутренних служб ОС Windows;

– анализ угроз и действий в системе в режиме реального времени;

– система информирования об угрозах;

– анализ и сбор данных в облачных и локальных сетях;

– сбор и ведение журнала событий.

Недостатки:

– система требовательна к вычислительным ресурсам;

– не всегда возможно оперативное устранение обнаруженных уязвимостей и багов.

Стоимость:

Стоимость одной бессрочной лицензии начинается от 1400 рублей. Для новых пользователей доступен 14-дневный пробный период.

DLP-системы

DLP-система (Data Leak Prevention) – специализированное ПО, созданное для защиты от утечек и кражи конфиденциальной корпоративной информации. DLP-системы используют технологию фильтрации и запрета на передачу данных через различные каналы и порты, которые могут быть небезопасны и уязвимы.

Рынок DLP-систем обширен и среди них выделяются и лидируют два программных продукта:

InfoWatch Traffic Monitor [62]

Данная система разработана для работ при больших нагрузках, если возникает необходимость обработки значительных массивов информации с целью ее обработки и анализа. Это ПО является масштабируемым и для крупных организаций и небольших офисов.

Основные возможности:

– обнаружение и анализ конфиденциального трафика всех типов;

– блокировка передачи конфиденциальной информации в случае нештатной ситуации или несанкционированного проникновения;

– предотвращение утечек информации сотрудниками организации;

– обнаружение и пресечение мошеннических схем, утечек данных;

– нахождение и предотвращение нестандартных угроз;

– контроль и анализ путей распространения информации внутри компании.

Недостатки:

– скудный функционал для контроля активности пользователей;

– отсутствие ПО для удаленного управления и отслеживания действий с компьютеров сотрудников;

– отсутствие целостной структуры из-за расположения разных модулей программы на разных серверах, что усложняет координацию действий между ними, настройку и поддержку ПО, а также создает дополнительные риски для организации и усложняет взаимодействие сотрудников с данными.

Стоимость:

InfoWatch – компания, нацеленная в основном на корпоративный сектор, потому что информация о программных решениях, ценах продуктов компании выдается исключительно по запросу от разработчика или покупателя в лице организации. Продукт продается с годовой лицензией. Стоимость зависит от используемой конфигурации.

DeviceLock DLP [58]

DeviceLock DLP – корпоративная система мониторинга информации и блокирования несанкционированных действий с ней. Приложение предоставляет пользователю широкие возможности, много функций для настройки сценариев действий и политик контроля. Это позволяет использовать данное программное решение в различных организациях разных типов с целью решения проблем информационной безопасности и надежной защиты конфиденциальных данных.

***Основные возможности*:**

– блокировка доступа пользователей различным видам данных;

– контроль и блокировка устройств;

– создание сценариев действий в различных ситуациях для противодействия несанкционированным действиям и контроля действий пользователей внутри сети;

– контроль доступа и взаимодействия пользователей с сетевыми ресурсами.

Недостатки:

– ограниченные возможности мониторинга сотрудников;

– отсутствие готовых сценариев и соответственно необходимость точной настройки сценариев для корректного срабатывания блокировки.

Стоимость:

Стоимость годичной лицензии начинается от 4 275 рублей. Более точная цена зависит от выбранной версии и конфигурации.

EveryTag [60]

EveryTag – программа, облегчающая поиски преступника, похитившего документы или данные. Она специальным образом обозначает документы, причем маркировка визуально незаметна. Поэтому это – цифровая метка. Если замечена утечка информации или появление измененной копии, ее можно загрузить в систему для того, чтобы узнать, кто украл информацию.

Основные возможности:

– защита электронных документов;

– защита от несанкционированного фото распечатанных документов;

– защита от несанкционированного съема документов с помощью снимков экрана;

– защита от хищения распечатанных документов.

Недостатки:

Это целевое ПО, так как его функционал позволяет лишь только обнаруживать сотрудников, похищающих документы.

***Стоимость*:**

Стоимость зависит от приобретаемой версии ПО. Стоимость разработчик предоставляет только по запросу клиента.

Корпоративные антивирусы

Система информационной безопасности организации не будет полноценной без внедрения хорошего корпоративного антивируса. Это программное решение для защиты информации и оборудования от воздействия вредоносного программного обеспечения, несанкционированного проникновения и хакерских атак.

Kaspersky Small Office Security [63]

Kaspersky Small Office Security – надежный антивирус, который постоянно обновляет базу данных и обеспечивает высокую защиту от различных видов угроз. Подходит для небольших компаний, но может использоваться также и в крупных организациях.

Основные возможности:

– файловый антивирус;
– сетевой антивирус;
– защита от сбора данных;
– контроль обновления программ;
– защита перехвата изображения с веб-камер;
– фильтрация активности пользователей;
– контроль установленных программ;
– защита банковской информации;
– блокировка рекламы;
– шифрование информации и трафика.

Недостатки:

– ПО больше ориентировано на малые офисы и предприятия;

– ограниченный функционал управления приложением.

Стоимость:

Стоимость годичной лицензии составляет от 3900 рублей для конфигурации с защитой до 5 ПК.

McAfee Endpoint Protection Essential [64]

Также очень популярным является корпоративный антивирус McAfee Endpoint Protect Essential. У него есть хороший набор инструментов для защиты от различных видов сетевых и программных угроз.

Основные возможности:

– брандмауэр;

– мониторинг в режиме реального времени;

– защита от вирусов-вымогателей;

– сетевая защита;

– контроль и анализ веб-трафика;

– автоматическая реакция на вероятные угрозы.

Недостатки:

– довольно сложная установка и настройка;

– данное ПО требовательно к вычислительным ресурсам.

***Стоимость*:**

Стоимость годичной лицензии составляет от 6000 рублей. Точная цена зависит от выбранной конфигурации.

Программные комплексы защиты загрузки и регистрации устройств, системы защиты информации

Secret Net Studio 8.5 [66]

Данное программное решение предназначено для решения следующих задач:

– защита конфиденциальной информации;

– защита от несанкционированного доступа и неправомерных действий преступника внутри информационных систем;

– соблюдение требований и рекомендаций, прописанных в нормативно-правовых актах, по обеспечению защиты данных в различных сегментах.

В данное ПО внедрены следующие функциональные возможности.

Шифрование контейнеров:

– данные на жестких дисках и внешних носителях хранятся в зашифрованном виде.

Контроль целостности данных:

– пересчет контрольных сумм данных и их сравнение с эталонными значениями;

– ведение журнала безопасности и оперативное уведомление администратора сети о нарушениях контура безопасности.

Создание «теневых» копий:

– при копировании информации на съемные носители, а также отправке документов на печать.

Гарантированное удаление данных:

– полное уничтожение секретной и закрытой информации без возможности восстановления даже за счет специализированных средств.

***Стоимость*:**

Стандартный набор ПО Secret Net Studio 8 со стандартной поддержкой, контролем устройств, встроенным антивирусом и межсетевым экраном – стоимость начинается от 6600 рублей за годовую лицензию.

Diamond ACS [59]

Система контроля и разграничения доступа Diamond ACS – кроссплатформенный программно-аппаратный комплекс защиты информации от неправомерного использования, сертифицированная в соответствии с действующим законодательством о информационной безопасности.

Основные возможности:

– системы управления и высокопроизводительное ядро клиентской части позволяют быстро реагировать на угрозы, а также справляться с возросшей ответственностью за безопасность;

– при использовании технологии Deep Virtual Secure достигается высокая степень изоляции выделенных контуров безопасности;

– кроссплатформенность;

– управление построено на определенном иерархическом принципе и поддерживает тесное взаимодействие со службами Microsoft Active Directory.

Аура [86]

«Аура» – это система защиты информации от несанкционированного доступа. Научная разработка и продукт Научного отдела проблем информационной безопасности Санкт-Петербургского института информатики, автоматики РАН.

Возможности данного ПО:

– наличие доверенной среды аутентификации, контроля целостности и настройки системы защиты информации вне защищаемой операционной системы. Усиленная аутентификации с помощью установки и использования «пароля на загрузку»;

– контроль целостности информационных объектов сетевой инфраструктуры;

– контроль доступа к устройствам, файлам и папкам;

– управление печатью, автоматическая маркировка и учет документов;

– прозрачное шифрование жестких дисков, съемного носителя и виртуального диска;

– качественное уничтожение информационных объектов;

– запись в журналы системной безопасности, передаваемые администратору сети;

– Rutoken осуществляет идентификацию и аутентификацию пользователей в доверенной среде с помощью электронных устройств;

– по таймауту система блокирует консоль и извлекает электронный ключ из нее при запуске защищенной операционной системы;

– смена пароля пользователя в операционной системе для управления доступом к сетевым ресурсам происходит автоматически;

– сессионный мандатный доступ.

Недостатки:

– недостаточно автоматизирован процесс настроек системы для использования разграничения доступа и замкнутой программной среды;

– мандатные метки на объекты файловой системы устанавливаются только лишь в файловой системе NTFS;

– разграничение доступа к устройствам действует на уровне шины по классам устройств, не идентифицируя конкретное устройство, подлежащее разрешению или запрету.

Стоимость:

Данное программное обеспечение для одной рабочей станции стоит от 7000 рублей, включая НДС, и стоимость установки и настройки.

Системы учета рабочего времени.

Kickidler [87] – программное решение для учета рабочего времени сотрудников. Организация не должна недооценивать изобретательность недобросовестных сотрудников, планирующих совершение корпоративных преступлений. Они регулярно придумывают и реализуют новые методы обхода систем защиты информации и ПО для контроля и блокировки движения информации. И на помощь руководству приходит подобное программное обеспечение.

Основные возможности:

– мониторинг ПК сотрудников в режиме реального времени;
– запись всех нажатий с клавиатуры;
– функция записи экрана в непрерывном режиме;
– регистрация и ведение журналов работы ПК каждого сотрудника;
– организация удаленного доступа к ПК сотрудников;
– оперативные уведомления о нарушениях на рабочем месте

Недостатки:

– отсутствие версий для мобильных корпоративных устройств;
– отсутствие синхронизации с облачными сервисами.

Стоимость:

Данное ПО существует в бесплатной версии (вплоть до 6 ПК). Доступен двухнедельный бесплатный пробный период для полной версии. Стоимость лицензии составляет 220 рублей в месяц за каждый подключенный ПК.

Таким образом, системы сбора данных контролируют поток информации в организации, ищут угрозы и предупреждают администраторов сети о них. Системы предотвращения утечек контролируют обмен данными и препятствуют их краже, а также несанкционированному доступу.

ПО для защиты документов исключает вероятность их кражи любым способом. Хороший корпоративный антивирус противодействует вирусному ПО,

сетевым атакам. Системы контроля и учета рабочего времени контролируют поведение и действия сотрудников.

Программно-аппаратные комплексы защиты информации включают в себя большой перечень настраиваемых компонентов и пакетов для обеспечения безопасности для одного отдельно взятого компьютера или компьютеров в сети. Вместе же все эти системы составляют защищенную информационную инфраструктуру организации, в которой сложно найти уязвимости и данные, а также тяжело уйти незамеченными нарушителям.

5.3. Программные средства и мероприятия по противодействию распространению вредоносных программ и взлома паролей

В современности, в процессе развития информационных технологий и технического прогресса, когда сложилось постиндустриальное общество, появилась новая проблема – защита персональных данных и паролей. Выделяется два основных способа противодействия. Первый способ основан на защите информации, система которой обеспечена независимостью от внешних факторов. Второй способ основан на защите информации, система которой устанавливает зависимость от данных процессов [55, с. 188].

Первое направление обеспечивает защиту и противодействие вредоносным программам, система которой постоянно обновляется, потому она является независимой. Преимуществом данного метода является эффективная функция распознавания вредоносных программ и их уничтожение.

Второе направление обеспечивает защиту данных посредством зависимости от происходящих процессов. Данная система не способная так эффективно организовывать структурированную концепцию безопасности.

Защита системы оснащена двухуровневой идентифицирующей базой, которая не позволяет чужеродным объектам распространять вирусные данные.

Базовую структуру защиты информации обеспечивают антивирусные программы, способные распознавать и уничтожать целостную структурную единицу вирусного объекта [57].

Фундаментальную защиту устройств и данных обеспечивает [75]:

1. Эвристическое сканирование.
2. СЯС-сканирование.
3. Антивирусный мониторинг.
4. Иммунизаторы.

Концепция деятельности и функционирования антивирусных сканеров базируется на проверке файлов, а также объектов, которые неизвестны сканеру. В последующем данные объекты заносятся в базу вредоносных программ, которые автоматически распознаются и уничтожаются. Указанный метод выявления дефектов программного обеспечения является более рациональным и эффективным.

Сканеры имеют свои разновидности и делятся на резидентные, осуществляющие сканирование в режиме реального времени, и нерезидентные, обеспечивающие проверку системы только по запросу [57].

Резидентные сканеры реализуют защиту системы, реагируют на появление вируса, в то время как нерезидентный сканер способен опознать вирус только во время своего очередного запуска программы. К достоинствам сканеров всех типов относится их универсальность, к недостаткам – размеры антивирусных баз, от чего зависит эффективность работы программ.

Прогрессивная работоспособность эвристического сканирования помогает проводить мониторинг и распознавать вредоносные программы, содержащие вирусы для сбоя в системе.

Поскольку эвристическое сканирование является во многом вероятностным методом поиска вредоносных программ, то на него распространяются многие законы теории вероятностей. Чем выше процент обнаруживаемых вирусов, тем больше количество ложных срабатываний.

Немаловажным является наблюдаемая в последнее время тенденция применения в эвристических сканерах их антивирусных баз, где хранится информация о характерных фрагментах кодов вредоносных программ.

Определенные антивирусные устройства созданы для распознавания вредоносных программ с помощью алгоритмов, заданных в программе (СЯС-сумм). Информация о контрольных суммах, а также данные о длине файлов, даты их последней модификации и т.д. сводится в базу данных и используется при последующих запусках СЯС-сканеров для сравнения с реально подсчитанными значениями.

Антивирусные мониторы – это резидентные программы, организующие наблюдательный процесс за вирусными программами. К преимуществу мониторов относится их способность распознавать вредоносные программы и оперативно их блокировать с последующим уничтожением, для обеспечения защиты встроенной компьютерной системы.

Развитие технологий позволяет разрабатывать новые варианты антивирусных программ с различными модификациями и новшествами, которые организуют достаточно эффективную систему безопасности BIOS-защиты.

Иммунизаторы – это программное обеспечение, которое способно создать имитацию зараженного файла вредоносной программой с целью тестирования и защиты реальной угрозы с последующим уничтожением. Основной задачей иммунизаторов является выработка живой системы защиты, которая сможет распознавать абсолютно любые элементы вирусных программ.

Большим минусом иммунизаторов является неспособность распознавать заражение вредоносной программой, использующей метод алгоритма, что требует определенной доработки модернизатором системы, для целостной и единой работы программы.

Систематика работы иммунизатора очень проста, но эффективна. При попытке вредоносной программы внедриться в файлы иммунизатор сообщает ей о том, что файлы уже заражены, и начинает обработку для уничтожения вредоносной программы.

Таким образом, можно сделать вывод, что защита компьютеров и телефонов обеспечивается только специализированными программными средствами и антивирусными программами, которые могут распознавать и противодействовать на автоматическом уровне вредоносным программам и попыткам взлома доступа к паролям.

В современном мире усиливается воздействие вредоносных программ, «заражающих» информационную систему, снимая с нее защиту, что угрожает утечкой информации, составляющей государственную тайну. Глобальной данная проблема является для военных баз и государственных систем. Для обеспечения защиты разрабатываются отечественные усовершенствованные программные инструменты по противодействию хакерским посягательствам.

Вопросы для самоконтроля:

1. С чем связан рост практического и научного интереса к проблематике киберпреступности?
2. Какой элемент киберпространства подвергается наибольшему риску угроз?
3. Что составляет основу большинства DDoS-атак?
4. В чем заключается специфика создания системы информационной безопасности предприятий и организаций?
5. Что представляют собой вирусы-шифровальщики?
6. Что в своей основе используют вирусы для реализации DDoS-атак?
7. В чем состоит базовый принцип обеспечения корпоративной информационной безопасности в современном мире?
8. Что входит в состав системного программного обеспечения защиты информации?
9. Что представляют собой DLP-системы?
10. Какие элементы входят в состав корпоративных антивирусов?

ЗАКЛЮЧЕНИЕ

В заключение можно сформулировать следующие основные выводы.

Рынок программного обеспечения для противодействия атакам на информационную инфраструктуру российских предприятий и корпораций насыщен большим количеством качественного ПО.

Каждая организация, от малой до крупной, независимо от размеров и располагаемых ресурсов на обеспечение необходимого уровня информационной безопасности сможет найти для себя подходящее решение для реализации своих задач.

До сих пор важнейшее значение имеет метод «совмещения» программных и аппаратных методов защиты, и подобные программно-аппаратные решения существуют и развиваются в соответствии с основными потребностями по обеспечению информационной безопасности в стране, в сотрудничестве с государственными органами.

Защитная инфраструктура должна постоянно обновляться по мере развития технологий, чтобы противостоять новым угрозам от хакеров. Ведь с каждым годом их становится все больше, и в будущем, если мы не озаботимся проблемами с информационной безопасностью, они смогут найти способы выводить из строя заводы, организации, государственные и социальные учреждения, что непременно окажет прямое влияние на качество жизни людей.

Эксперты прогнозируют большой рост рынка обеспечения информационной безопасности [75]. Государство сейчас делает все возможное, чтобы новые специалисты появлялись в этой отрасли все чаще и в большом количестве [2]. Открываются новые специальности в высших и средних учебных заведениях, создаются курсы по информационной безопасности, обычных людей учат цифровой грамотности и правилам использования сети Интернет так, чтобы это приносило только пользу, а не вред.

Каждому стоит озаботиться собственной информационной безопасностью, чтобы не стать жертвой хакерских атак, а также чтобы не потерять данные, финансы.

Даже простое использование обычного домашнего антивируса поможет снизить риск подхватить большую часть серьезных вирусов, а встроенная защита в браузере поможет избежать попадания на небезопасные сайты. Также стоит проверять USB-накопители на наличие вирусов и не использовать неизвестные носители [42, с. 591].

Материалы пособия могут найти применение в преподавании дисциплин «Информатика и информационные технологии в профессиональной деятельности» по направлению подготовки 40.05.01 «Правовое обеспечение национальной безопасности», «Информационно-коммуникационные технологии в профессиональной служебной деятельности» по направлению подготовки 40.03.02 «Обеспечение законности и правопорядка», в том числе с использованием дистанционных технологий посредством электронной образовательной среды института.

Библиографический список

1. ГОСТ Р 56824-2015. Национальный стандарт Российской Федерации. Интеллектуальная собственность. Использование охраняемых результатов интеллектуальной деятельности в сети Интернет: утв. и введен в действие приказом Росстандарта от 03.12.2015 №2103-ст // Стандартинформ, 2017.
2. Указ Президента Российской Федерации от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» // СПС «КонсультантПлюс».
3. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 18.02.2020) // Собрание законодательства Российской Федерации. 1996. № 25. Ст. 2954.
4. Приказ МВД России от 10.05.2018 № 284 «Об утверждении плана-графика перехода Министерства внутренних дел Российской Федерации на использование отечественного офисного программного обеспечения на 2018 год и на плановый период до 2020 года» // База данных «Нормативно-правовые акты МВД России».
5. Акапьев В.Л. Формирование информационно-технологической компетентности сотрудников ОВД: монография. – Белгород: Белгородский юридический институт МВД России имени И.Д. Путилина, 2015. – 189 с.
6. Акапьев В.Л. [и др.] Практико-ориентированное обучение информационным технологиям в рамках внедрения свободного программного обеспечения в органах внутренних дел. – Белгород: Белгородский юридический институт МВД России имени И.Д. Путилина, 2022. – 120 с.
7. Амельчаков И.Ф. [и др.] Информатика и информационные технологии в профессиональной деятельности: учебник. – Белгород: Бел ЮИ МВД России имени И.Д. Путилина, 2018. – 369 с.
8. Бабаш А.В. Информационная безопасность и защита информации: учебное пособие. – Москва: РИОР, 2022. – 336 с.
9. Вострецова Е.В. Основы информационной безопасности: учебное пособие для студентов вузов. – Екатеринбург: Урал. ун-т, 2019. – 204 с.
10. Зенков А.В. Информационная безопасность и защита информации: учебное пособие. – Москва: Юрайт, 2022. – 104 с.
11. Кесарева Т.П. Криминологическая характеристика и проблемы предупреждения преступности в российском сегменте сети Интернет: дис. ... канд. юрид. наук. – Москва, 2002. – 195 с.
12. Киберпреступность: риски и угрозы: материалы Всероссийского студенческого круглого научно-практического стола с международным участием (Северо-Западный филиал ФГБОУВО «Российский государственный университет правосудия» (Санкт-Петербург, 11 февраля 2021 г.) / под ред. д-ра юрид. наук, доцента Е.Н. Рахмановой. – Санкт-Петербург: Астерион, 2021. – 236 с.
13. Дубоносов Е.С. Оперативно-розыскная деятельность – Москва: Юрайт, 2017. – 379 с.

14. Панфилова Е.И., Попов А.Н. Компьютерные преступления. Серия «Современные стандарты в уголовном праве и уголовном процессе» / науч. ред. проф. Б.В. Волженкин. – Санкт-Петербург: Институт Генеральной прокуратуры Российской Федерации, 1998. – 48 с.

15. Преступления в сфере обращения цифровой информации / И.Р. Бегишев, И.И. Бикеев. – Казань: Познание, 2020. – 300 с.

16. Савотченко С.Е. Частные методики образовательных технологий формирования информационно-технологической компетентности сотрудников правоохранительных органов: учебно-методическое пособие. – Белгород: Белгородский юридический институт МВД России имени И.Д. Путилина, 2018. – 68 с.

17. Смирнова Т.Г. Уголовно-правовая борьба с преступлениями в сфере компьютерной информации: автореф. дис. ... канд. юрид. наук. – Москва, 1998. – 161 с.

18. Акапьев В.Л., Савотченко С.Е. Актуальные проблемы импортозамещения программного обеспечения образовательных организаций в контексте информационной безопасности // Дистанционное и виртуальное обучение. 2015. № 11. С. 113–125.

19. Акапьев В.Л. [и др.] Детализация информационной компетентности сотрудников органов внутренних дел / Проблемы информационного обеспечения деятельности правоохранительных органов: сборник статей 3-й Международной научно-практической конференции (14 октября 2016 г.). – Белгород: Белгородский юридический институт МВД России имени И.Д. Путилина, 2017. С. 174–179.

20. Акапьев В.Л. [и др.] Информационные технологии в обеспечении экономической безопасности / Математические методы и информационно-технические средства: материалы XVI Всероссийской научно-практической конференции, 19 июня 2020 г. – Краснодар: Краснодарский университет МВД России, 2020. С. 6–10.

21. Акапьев В.Л., Савотченко С.Е. Нормативно-правовые аспекты регулирования цифровой образовательной среды. Право и образование. 2020. № 4. С. 32–38.

22. Акапьев В.Л. Правовые аспекты противодействия использованию баз персональных данных в преступных и противоправных целях / Актуальные проблемы правоохранительной деятельности органов внутренних дел на современном этапе (300-летию российской полиции посвящается): материалы Всероссийской научно-практической конференции. – Казань: Казанский юридический институт МВД России, 2018. С. 67–71.

23. Акапьев В.Л. [и др.] Профилактическая деятельность органов внутренних дел во взаимодействии со средствами массовой информации // Вестник Воронежского института МВД России. 2018. № 2. С. 146–252.

24. Акапьев В.Л. [и др.] Система правового регулирования в области создания, использования и хранения баз данных / 300 лет на страже закона и правопорядка: материалы Всероссийской научно-практической конференции. – Хабаровск: Дальневосточный юридический институт МВД России, 2018. С. 110–114.

25. Акапьев В.Л. Системный анализ понятия профессиональной компетентности / Проблемы информационного обеспечения деятельности правоохранительных органов: сборник статей 3-й Международной научно-практической конференции (Белгород, 14 октября 2016 г.). – Белгород: Белгородский юридический институт МВД России имени И.Д. Путилина, 2017. С. 167–172.

26. Акапьев В.Л. [и др.] Совершенствование контроля и устранения нарушений законности при осуществлении приема, регистрации и проверки сообщений о преступлениях // Вестник Воронежского института ФСИН. 2018. № 1. С. 131–138.

27. Акапьев В.Л. Некоторые аспекты использования СПО в образовательных организациях системы МВД России / Современные информационные технологии в профессиональной деятельности сотрудников органов внутренних дел: сборник материалов Всероссийской научно-теоретической конференции (22 апреля 2022 г.) – Ростов-на-Дону: Ростовский юридический институт МВД России, 2022. С. 20–27.

28. Акапьев В.Л. [и др.] Практико-ориентированное обучение информационным технологиям в рамках внедрения свободного программного обеспечения в органах внутренних дел / Современные информационные технологии в профессиональной деятельности сотрудников органов внутренних дел: сборник материалов Всероссийской научно-теоретической конференции (22 апреля 2022 г.). – Ростов-на-Дону: Ростовский юридический институт МВД России, 2022. С. 4–11.

29. Бронников Д.А. Сравнительное исследование законодательства стран ЕАЭС в части противодействия ИТ-преступлениям в сфере экономики // Вестник экономической безопасности. 2021. С. 103–108.

30. Быков В.М. Преступления в сфере компьютерной информации // Российский судья. 2022. № 3. С. 32–54.

31. Васильков Е.Д. Уголовно-правовая характеристика преступлений, совершенных с использованием информационных технологий // StudNet. 2021. № 6. С. 10–15.

32. Верещагина А.В. К вопросу о предмете неправомерного доступа к компьютерной информации // Территория новых возможностей. Вестник Владивостокского государственного университета экономики и сервиса. 2020. № 2. С. 103–117.

33. Вехов В.Б. Преступления в сфере цифровой экономики: совершенствование расследования на основе положений электронной криминалистики // Пермский юридический альманах. Право. 2019. № 1. С. 128–136.

34. Власова С.В. К вопросу о приспосабливании уголовно-процессуального механизма к цифровой реальности // Библиотека криминалиста. 2018. № 1 (36). С. 14–15.

35. Волеводз А.Г. Борьба с киберпреступностью // Методики реализации. 2022. № 5. С. 22–24.

36. Воробьев А.В. Латентность преступлений против личности в исправительных учреждениях УИС // Теория и практика социогуманитарных наук. 2021. № 2(14). С. 74–76.

37. Головин А.Ю., Давыдов В.О. Значение виртуальных следов в расследовании преступлений экстремистского характера // Известия Тульского государственного университета. Экономические и юридические науки. 2016. № 3–2. С. 254–259.

38. Гончар В.В. Анализ состояния расследования киберпреступлений следственными подразделениями МВД России в 2019 году // Научный компонент. 2020. № 3(7). С. 238–244.

39. Грибунов О.П. К вопросу о противодействии экстремизму на объектах транспорта // Вестник Восточно-Сибирского института МВД России. 2013. № 3(66). С. 9–16.

40. Дрога А.А. [и др.] Проблемы обеспечения информационной безопасности мобильных устройств в правоохранительных органах / Математические методы и информационно-технические средства: материалы XVI Всероссийской научно-практической конференции (18 июня 2021 г.). – Краснодар: Краснодарский университет МВД России, 2021. С. 44–50.

41. Запечников С.В. Угрозы, уязвимости, атаки и подходы к защите // Информационная безопасность открытых систем. 2022. № 6. С. 25–44.

42. Зуев С.В., Никитин Е.В. Информационные технологии в решении уголовно-процессуальных проблем // Всероссийский криминологический журнал. 2017. Т. 11. № 3. С. 587–595.

43. Иванцов С.В., Молчанова Т.В. Информационно-телекоммуникационные технологии – современная реальность преступности // Вестник Санкт-Петербургского университета МВД России. 2020. № 4(88). С. 89–96.

44. Прокопенко А.Н. [и др.] Особенности осуществления правоохранительными органами мероприятий по противодействию информационным угрозам в социальных сетях // Вестник Краснодарского университета МВД России. 2018. № 4(42). С. 55–61.

45. Савотченко С.Е., Прокопенко А.Н. Использование социальных сетей в противоправных целях // Наука. Культура. Искусство: актуальные проблемы теории и практики: сборник докладов Международной научно-практической конференции (21 марта 2018 г.): в 4-х т. – Белгород: Белгородский государственный институт искусств и культуры, 2018. Т. 1. С. 99–103.

46. Савотченко С.Е. [и др.] Критерии использования социальных сетей в образовательной деятельности // Открытое и дистанционное образование. 2019. № 1(73). С. 53–60.

47. Савотченко С.Е. [и др.] Характеристики и разновидности интернет-преступлений и их развитие / Проблемы информационного обеспечения деятельности правоохранительных органов: сборник статей V международной научно-практической конференции. – Белгород: Белгородский юридический институт МВД России имени И.Д. Путилина, 2019. С. 46–53.

48. Савотченко С.Е. [и др.] Системный поход к обеспечению информационной и экономической безопасности хозяйствующего субъекта / Проблемы информационного обеспечения деятельности правоохранительных органов: сборник статей 9-й Всероссийской научно-практической конференции, 20 мая

2022 г. – Белгород: Белгородский юридический институт МВД России имени И.Д. Путилина. 2022. С. 142–146.

49. Савотченко С.Е. [и др.] Правовые и организационные проблемы реализации информационной безопасности детей в Российской Федерации // Право и образование. 2022. № 11. С. 52–63.

50. Савотченко С.Е. Профилактика преступлений в сфере информационных технологий // Алтайский юридический вестник. 2022. № 4(40). С. 84–89.

51. Савотченко С.Е. [и др.] Особенности реализации электронного документооборота в информационном пространстве образовательных организаций // Открытое и дистанционное образование. 2022. № 2(82). С. 21–26.

52. Тимофеев С.В. Информационное обеспечение противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий // Известия Тульского государственного университета. Экономические и юридические науки. 2021. С. 132–137.

53. Унукович А.С. Понятие преступлений, совершаемых с использованием информационно-телекоммуникационных технологий // Государственная служба и кадры. 2021. № 4. С. 278–280.

54. Хисамова З.И. Об особенностях квалификации преступлений, совершаемых в сфере использования информационно-коммуникационных технологий // Общество и право. 2016. № 1(55). С. 117–120.

55. Шевко Н.Р., Казанцев С.Я. Кибербезопасность: проблемы и пути решения // Вестник экономической безопасности. Юридические науки. 2020. № 5. С. 186–189.

56. Шкеле М.В. Проблемы квалификации преступлений, совершенных с использованием информационных технологий / Уголовное законодательство: вчера, сегодня, завтра: материалы ежегодной всероссийской научно-практической конференции. – Санкт-Петербург: Санкт-Петербургский университет МВД России, 2021. Ч. 1. С. 266–271.

57. «Код Безопасности» [Электронный ресурс]. – Режим доступа: https://www.securitycode.ru/calc/#open/calc/calc-sns (дата обращения: 05.05.2022).

58. DeviceLock DLP [Электронный ресурс]. – Режим доступа: https://www.acronis.com/en-us/products/devicelock/ (дата обращения: 11.05.2022).

59. Diamond ACS – комплекс защиты информации от НСД» [Электронный ресурс]. – Режим доступа: http://tss-test.herokuapp.com/products/diamond_acs#benefits (дата обращения: 05.05.2022).

60. EveryTag [Электронный ресурс]. – Режим доступа: https://everytag.ru (дата обращения: 11.05.2022).

61. IBM Security QRadar SIEM. [Электронный ресурс]. – Режим доступа: https://www.ibm.com/qradar/security-qradar-siem (дата обращения: 05.05.2022).

62. InfoWatch Traffic Monitor [Электронный ресурс]. – Режим доступа: https://infowatch.com/products/traffic_monitor_enterprise (дата обращения: 11.05.2022).

63. Kaspersky Small Office Security [Электронный ресурс]. – Режим доступа: https://www.kaspersky.com/small-business-security/small-office-security (дата обращения: 11.05.2022).

64. McAfee Endpoint Protection Essential [Электронный ресурс]. – Режим доступа: https://store.softline.ru/mcafee/mcafee-endpoint-protection-essential-for-smb/ (дата обращения: 11.05.2022).

65. McAfee Enterprise Security Manager [Электронный ресурс]. – Режим доступа: https://www.mcafee.com/enterprise/ru-ru/products/enterprise-security-manager/support.html (дата обращения: 11.05.2022).

66. Secret Net Studio 8.5 для защиты данных и IT-инфраструктуры [Электронный ресурс]. – Режим доступа: https://www.securitycode.ru/products/secret-net-studio/ (дата обращения: 11.05.2022).

67. Splunk Enterprise Security [Электронный ресурс]. – Режим доступа: https://ib.radiuscompany.ru/products/splunk-enterprise-security/ (дата обращения: 11.05.2022).

68. WannaCry [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/WannaCry (дата обращения: 11.05.2022).

69. Анализ мирового и отечественного опыта внедрения фондов алгоритмов и программ, разработанных документов [Электронный ресурс]. – Режим доступа: linuxformat.ru/ download/foss-russia/3.1 (дата обращения: 02.09.2021).

70. Анализ российского рынка информационной безопасности [Электронный ресурс]. – Режим доступа: https://www.anti-malware.ru/analytics/Market_Analysis/Russian-InfoSec-Market (дата обращения: 05.03.2022).

71. Белоусов А. Компьютерная программа как объект защиты авторского права [Электронный ресурс]. – Режим доступа: https://crime-research.ru/library/Belous1203.html (дата обращения: 19.02.2022).

72. Волков Д. Платформа национальной безопасности [Электронный ресурс]. – Режим доступа: osp.ru/news/articles/2011/46/13011311/ (дата обращения: 02.09.2021).

73. Гордейчик С. Бесплатно и безопасно: главные мифы свободного ПО [Электронный ресурс]. – Режим доступа: habrahabr.ru/company/pt/blog/249927 (дата обращения: 02.09.2021).

74. Информационная безопасность (мировой рынок) [Электронный ресурс]. – Режим доступа: https://goo.su/QTfpC (дата обращения: 05.03.2022).

75. Исследование российского рынка информационной безопасности [Электронный ресурс]. – Режим доступа: https://www.securitycode.ru/upload/iblock/ (дата обращения: 11.03.2022).

76. Киберпреступлений становится все больше, однако их раскрываемость уменьшается / Адвокатская газета: офиц. сайт органа Федеральной палаты адвокатов Российской Федерации [Электронный ресурс]. – Режим доступа: https://www.advgazeta.ru/novosti/kiberprestupleniy-stanovitsya-vse-bolshe-odnako-ikh-raskryvaemost-umenshaetsya/ (дата обращения: 28.03.2022).

77. Киберпреступность в глобальной информационной сети / StudRef [Электронный ресурс]. – Режим доступа: https://studref.com/306274/informatika/kiberprestupnost_globalnoy_informatsionnoy_seti (дата обращения: 19.02.2022).

78. Киберпреступность глазами студентов Амурского колледжа строительства и жилищно-коммунального хозяйства / Информио [Электронный ресурс]. – Режим доступа: https://www.informio.ru/ (дата обращения: 28.03.2022).

79. Компетентностный подход в образовании [Электронный ресурс] – Режим доступа: http://biofile.ru/psy/11508.html (дата обращения: 02.10.2022).

80. Компетентностный подход в профессиональном образовании [Электронный ресурс] – Режим доступа: http://www.syl.ru/article/173512/new (дата обращения: 04.09.2022).

81. Постановление Пленума Верховного Суда Российской Федерции от 26.12.2017 № 57 «О некоторых вопросах применения законодательства, регулирующего использование документов в электронном виде в деятельности судов общей юрисдикции и арбитражных судов» // Доступ из Базы данных «Нормативно-правовые акты МВД России».

82. Основы обеспечения информационной безопасности [Электронный ресурс]. – Режим доступа: https://itssupport.ru/blog/osnovyi-obespecheniya-informaczionnoj-bezopasnosti.html (дата обращения: 12.03.2022).

83. ПО для защиты информации (мировой рынок) [Электронный ресурс]. – Режим доступа: https://goo.su/CM4DF (дата обращения: 05.03.2022).

84. По цифровым следам: в Российской Федерации раскрывается лишь четверть киберпреступлений / Securitylab [Электронный ресурс]. – Режим доступа: https://www.securitylab.ru/blog/company/CABIS/347590.php (дата обращения: 30.03.2022).

85. Свободное программное обеспечение в госорганах [Электронный ресурс]. – Режим доступа: http://bda-expert.com/ (дата обращения: 02.09.2021).

86. Система защиты информации «Аура» [Электронный ресурс]. – Режим доступа: https://cobra.ru/prod/aura (дата обращения: 11.05.2022).

87. Система контроля и учета рабочего времени сотрудников «Kickidler» [Электронный ресурс]. – Режим доступа: https://www.kickidler.com (дата обращения: 11.05.2022).

88. Систематизация подходов формирования профессиональной компетентности [Электронный ресурс] – Режим доступа: http://studopedia.ru/15_115164_sistematizatsiya-podhodov-formirovaniya-professionalnoy-kompetentnosti.html (дата обращения: 02.09.2021).

89. Следственный комитет / Официальный сайт [Электронный ресурс]. – Режим доступа: https://sledcom.ru/news/item/ (дата обращения: 08.03.2022).

90. Судебная практика по компьютерным преступлениям (краткий обзор) / Интернет и право: официальный сайт юридической фирмы [Электронный ресурс]. – Режим доступа: https://internet-law.ru/intlaw/crime/sudebnaya-praktika-po-kompyuternim-prestupleniyam.htm (дата обращения: 10.03.2022).

91. Судебные и нормативные акты Российской Федерации / Судебные и нормативные акты Российской Федерации (СудАкт) [Электронный ресурс]. – Режим доступа: https://sudact.ru/ (дата обращения: 10.03.2022).

92. Число киберпреступлений в России / TADVISER [Электронный ресурс]. – Режим доступа: https://www.tadviser.ru/index.php/ (дата обращения: 12.04.2022).

УЧЕБНОЕ ИЗДАНИЕ

Дрога Андрей Анатольевич,
Савотченко Сергей Евгеньевич,
доктор физико-математических наук, доцент
Акапьев Виктор Львович,
кандидат педагогических наук, доцент

Использование особенностей системного программного обеспечения для противодействия преступности в сфере информационно-телекоммуникационных технологий

Учебное пособие

Редактор *О.Н. Тулина*
Комп. верстка *И.Ю. Чернышева*

Подписано в печать 2023. Формат 60x90/16
Усл. печ. л. 3 Тираж 74 экз. Заказ 21

Отпечатано в отделении полиграфической и оперативной печати
Белгородского юридического института МВД России имени И.Д. Путилина
г. Белгород, ул. Горького, 71

ISBN 978-5-91776-484-9