Содержание:

Введение

Актуальность темы исследования. Изменения, происходящие в социально-экономической и политической сферах жизни Казахстана — рост информационного обмена в стране и мире, создание финансово-кредитной системы и предприятий различных форм собственности, а также переход общества на расчеты с помощью «электронных денег» и т. д., — оказывают существенное влияние на вопросы защиты информации. Долгое время в нашей стране существовала только одна собственность — государственная, поэтому информация и секреты были тоже только государственными, охраняемые мощными спецслужбами. С ростом информационного обмена в пространстве особую значимость приобретает проблема защиты конфиденциальной информации — банковской, налоговой, коммерческой.

Широкое использование современных информационных технологий в управленческих и финансовых структурах, а также в обществе в целом выдвигает решение проблемы информационной безопасности в число приоритетных задач. Это дает основание введения в национальную систему права отдельной отрасли такой как информационное или компьютерное право, одним из основных аспектов которой являются т. н. компьютерные посягательства. Кроме того, об актуальности проблемы свидетельствует обширный перечень возможных способов компьютерных преступлений. В этой связи приняты государственные программы обеспечения информационной безопасности, обеспечения защиты государственных секретов, Концепция обеспечения информационной безопасности, а также ряд других организационных и практических мер, которые реализуются государственными органами Республики Казахстан во взаимодействии с Комитетом национальной безопасности.

Каждый сбой работы компьютерной сети — это не только «моральный» ущерб для работников предприятий и сетевых администраторов. По мере развития технологий электронных платежей, «безбумажного» документооборота и других, серьезный сбой локальных сетей может парализовать работу целых корпораций и банков, что приводит к ощутимым материальным потерям. Не случайно то, что защита данных в компьютерных сетях становится одной из самых острых проблем

в современной информатике. На сегодняшний день сформулировано три базовых принципа информационной безопасности: целостность данных — защита от сбоев, ведущих к потере информации, а также неавторизованного создания или уничтожения данных; конфиденциальность информации и, одновременно, ее доступность для всех авторизованных пользователей. Следует также отметить, что отдельные сферы деятельности (банковские и финансовые институты, информационные сети, системы государственного управления, оборонные и специальные структуры) требуют специальных мер по обеспечению безопасности данных и предъявляют повышенные требования к надежности функционирования информационных систем, в соответствии с характером и важностью решаемых ими задач.

Указанные обстоятельства предопределили выбор темы и актуальность данного исследования, а рассматриваемые вопросы имеют большое теоретическое и практическое значение.

Цель и задачи исследования. Целью настоящего исследования является изучение технологий совершения компьютерных преступлений.

В соответствии с целью исследования были поставлены следующие задачи:

- раскрыть содержание понятий «компьютерная преступность», «преступления в сфере информационных технологий»;
- проанализировать технологии компьютерной преступности;
- рассмотреть технологии борьбы с компьютерной преступностью;
- выявить проблемы, возникающие в процессе компьютерных преступлений.

Глава 1. Сущность и технологии компьютерной преступности

1.1 Понятие компьютерных преступлений

XXI в. — век стремительного прогресса информационных технологий. Так, в 2019 г. на Интернет-экономику в мире уже приходилось около 25 % валового продукта. Объем передаваемых данных через Интернет удваивается, что, на наш взгляд, указывает на появление реальной зависимости развитых стран мира от

международной информационной инфраструктуры. Несомненно, это затронуло и Казахстан.

Однако на сегодняшний день Интернет выступает не только как кладезь информации, но и как угроза в виде информационных войн и компьютерной преступности. При этом выделяется пять основных направлений правового регулирования Интернет-отношений:

1. защита личных данных и частной жизни в сети Интернет;
2. регулирование электронной коммерции и иных сделок и обеспечение их безопасности;
3. защита интеллектуальной собственности;

4) борьба против противоправного содержания информации и противоправного поведения в сети;

5) правовое регулирование электронных сообщений.

Для того чтобы сформулировать понятие компьютерной преступности необходимо дать определение понятию компьютерного преступления.

С необходимостью разработки понятия преступлений в сфере компьютерной информации и определения их места в системе уголовного законодательства ученые столкнулись задолго до появления этих деяний в качестве отдельных составов преступлений, то есть до принятия ныне действующего Уголовного кодекса Республики Казахстан.

Первое научное обсуждение компьютерной преступности было осуществлено в 1993 г. на семинаре «Криминалистика и компьютерная преступность» научно-исследовательского института проблем укрепления законности и правопорядка Генеральной прокуратуры РФ и ЭКЦ МВД России, где В. Н. Дре-миным было предложено компьютерные преступления толковать как «предусмотренные законом общественно опасные действия, в которых машинная информация является либо средством, либо объектом преступного посягательства». При этом указанное понятие не содержало упоминания о виновном характере посягательств, а также последствий или возможности их наступления в результате совершения общественно опасного деяния.

В литературе на данный счет мнения ученых разделились.

Так, по мнению В. Б. Вехова, «под компьютерными преступлениями нужно понимать предусмотренные уголовным законом общественно опасные действия, в которых машинная информация является объектом преступного посягательства» [1, с. 23].

А. К. Караханьян считает, что к компьютерным преступлениям относится «внесение изменений в информацию на различных этапах ее обработки в программное обеспечение, а также овладение информацией» [2, с. 244].

К. С. Скоромников, говоря о частом использовании термина «компьютерные преступления» в правоприменительной практике в отношении общественно опасных деяний с применением средств вычислительной техники и об отсутствии данного термина в уголовном законодательстве, предлагает ввести его в официальную судебную статистику как условное наименование компьютерных преступлений [3, с. 168]. Мы не согласны с таким предложением, так как в рассматриваемой сфере появляются новые деяния, которые осуществляются не только посредством ЭВМ, системы ЭВМ или их сети, но и с помощью теле-коммуникационного оборудования.

При этом в уголовно-правовой литературе существовало две позиции, это когда одни ученые предлагали именовать рассматриваемые деяния компьютерными преступлениями, другие — преступлениями в сфере компьютерной информации.

Например, С. В. Бородин и А. В. Наумов рассматривают преступления в сфере компьютерной информации как общественно опасные деяния, которые «конкретно направлены против той части установленного порядка общественных отношений, который регулирует изготовление, использование, распространение и защиту компьютерной информации» [4, с. 662]. При этом они не указывают на последствия и на форму вины рассматриваемых преступлений, отмечая только, что объектом преступления выступают интересы личности, общества, государства, охраняемые уголовным законом в области безопасности изготовления, использования и распространения компьютерной информации, информационных ресурсов, систем и технологий.

Т. Г. Смирнова рассматривает преступления в сфере компьютерной информации как «запрещенные уголовным законом общественно опасные деяния, которые, будучи направленными на нарушение неприкосновенности охраняемой законом компьютерной информации и ее материальных носителей, причиняют либо сохраняют угрозу причинения вреда жизни и здоровью личности, праваи и

свободам человека и гражданина, государственной и общественной безопасности» [5, с. 14].

При этом необходимо различать машинную информацию, то есть информацию, являющуюся продуктом, произведенным с помощью или для компьютерной техники (например, программа для управления устройствами ЭВМ), и информацию, имеющую «некомпьютерный» характер (например, электронный документ) [6, с. 17].

Под машинной информацией понимается информация, циркулирующая в вычислительной среде, зафиксированная на физическом носителе в форме, доступной восприятию ЭВМ, или передающаяся по телекоммуникационным каналам, сформированная в вычислительной среде и пересылаемая посредством электромагнитных сигналов из одной ЭВМ в другую, из ЭВМ на периферийное устройство либо на управляющий датчик оборудования.

Также необходимо учитывать, что компьютер в преступлениях может выступать в качестве предмета и орудия совершения преступления. Данное свойство определяется технологической спецификой его строения.

На X Конгрессе ООН по предупреждению преступности и обращению с правонарушителями, компьютерные преступления были подразделены на две категории:

1. любое противоправное деяние, совершенное посредством электронных операций, целью которого является безопасность компьютерных систем и обрабатываемых ими данных (в узком смысле);
2. любое противоправное деяние, совершенное посредством или связанное с компьютерами, компьютерными системами или сетями, включая незаконное владение и предложение или распространение информации посредством компьютерных систем или сетей (в широком смысле, как преступление, связанное с компьютерами)[7].

В США используются, например, такие понятия как «Heiterkcrime» или «Kibercrime», означающие «преступления в сфере высоких технологий» и «ки-берпреступления». В действующем уголовном законодательстве Республики Казахстан данный вид преступных деяний определен как преступления в сфере компьютерной информации. На наш взгляд, указанное название не дает возможности четко определить конкретный вид преступлений, что приводит к неоднозначности, потому что необходимо учитывать тот факт, что компьютеры используются

практически во всех сферах жизнедеятельности общества и являются лишь одной из разновидностей информационного оборудования. По нашему мнению, данные преступления целесообразно обозначить как преступления, совершенные в сфере информационных технологий — предусмотренные уголовным законом виновные общественно опасные деяния, направленные на нарушение неприкосновенности охраняемой законом электронной информации и ее материальных носителей, совершаемые в процессе создания, использования и распространения электронной информации, а также направленные на нарушение работы ЭВМ, системы ЭВМ или их сети, причиняющие вред законным интересам собственников или владельцев, жизни и здоровью личности, правам и свободам человека и гражданина, национальной безопасности, где предметом выступает компьютерная информация.

Таким образом, сформулировав определение понятия преступлений в сфере информационных технологий возможно определить компьютерную преступность, как **совокупность преступлений в сфере компьютерной информации и опосредованных общественно опасных деяний.** Сосуществование этих общественно опасных деяний способно причинить значительный вред интересам личности, общества и государства, они посягают на безопасность компьютерной информации.

Подпадая под определение преступности вообще, компьютерная преступность является профессиональной по следующим признакам:

1. Наличие у преступника определенных познаний и навыков во владении компьютерной техникой.
2. Устойчивый вид преступного занятия.
3. Совершение данного вида преступления как источник средств существования или получения выгоды.
4. Наличие устойчивых связей с антисоциальной средой.
5. Совокупность профессиональных преступников, что свидетельствует о масштабности преступной деятельности в сфере информационных технологий.

Таким образом, компьютерная преступность представляет собой естественный и необходимый результат эволюции общества, основанный на информационных технологиях, выступает как дополнительная комфортная форма жизнедеятельности, не поддающаяся ликвидации либо преодолению и требующая адекватных способов и методов регулирования и управления в целях минимизации причиняемого вреда интересам личности, общества и государства, обладающее

признаками профессиональной преступности и представляющее собой виновное нарушение уголовно-правовых запретов и совокупность всех фактически совершенных преступлений в сфере информационных технологий.

На наш взгляд, к компьютерной преступности примыкают и некоторые действия, направленные на поддержание условий для ее существования и развития (например, создание сайтов, направленных на распространение криминальной идеологии, а также обмен криминальным опытом и специальными познаниями). В сети Интернет насчитывается более 30 тысяч ориентированных на взлом сайтов, где любое лицо может приобрести за небольшую сумму книгу, обучающую элементарным приемам атаки на информационные системы [24].

1.2 Виды компьютерных правонарушений

С целью унификации национальных законодательств в 1989 г. комитетом министров Европейского союза был согласован и утвержден Список правонарушений, рекомендованный странам-участницам ЕС для разработки единой уголовной стратегии, связанной с компьютерными преступлениями.

«Минимальный список нарушений» содержит следующие восемь видов компьютерных преступлений:

1. **Компьютерное мошенничество.** Ввод, изменение, стирание или повреждение данных ЭВМ или программ ЭВМ, или же другое вмешательство в ход обработки данных, которое влияет на ход обработки данных таким образом, что служит причиной экономических потерь или вызывает состояние потери имущества другого человека с намерением незаконного улучшения экономического положения для себя или другого человека (как альтернатива — с намерением к незаконному лишению этого человека его имущества).
2. **Подделка компьютерной информации.** Несанкционированное стирание, повреждение, ухудшение или подавление данных ЭВМ, или другое вмешательство в ход обработки данных различными способами, или создание таких условий, которые будут, согласно национальному законодательству, составлять такое правонарушение, как подделка в традиционном смысле такого нарушения.
3. **Повреждение данных ЭВМ или программ ЭВМ.** Несанкционированное стирание, повреждение, ухудшение или подавление данных ЭВМ или программ

ЭВМ.

4. **Компьютерный саботаж.** Ввод, изменение, стирание, повреждение данных ЭВМ или вмешательство в системы ЭВМ с намерением препятствовать функционированию компьютера или системы передачи данных.

5. Несанкционированный доступ к системе ЭВМ через сеть с нарушением средств защиты.

1. **Несанкционированный перехват данных** с помощью технических средств связи как в пределах компьютера, системы или сети, так и извне.
2. **Несанкционированное использование защищенных компьютерных программ.** Незаконное воспроизведение, распространение или связь с программой ЭВМ, которая защищена в соответствии с законом.
3. **Несанкционированное воспроизведение схем.** Несанкционированное воспроизведение схемных решений, защищенных в соответствии с законом о полупроводниковых изделиях (программах), или коммерческая эксплуатация, или незаконное импортирование для той же цели схемы или полупроводникового изделия как продукта, произведенного с использованием данных схем.

«Необязательный список нарушений» включает в себя следующие четыре вида компьютерных преступлений:

1. **Изменение данных ЭВМ или программ ЭВМ.** Незаконное изменение данных или программ ЭВМ.
2. **Компьютерный шпионаж.** Приобретение с использованием незаконных средств или путем несанкционированного раскрытия, пересылка или использо-
   вание торговых или коммерческих секретов при помощи подобных методов или других незаконных средств с тем или иным намерением, наносящим экономический ущерб человеку путем доступа к его секретам или позволяющим получить незаконное экономическое преимущество для себя или другого человека.
3. **Неразрешенное использование ЭВМ.** Использование системы ЭВМ или компьютерной сети без соответствующего разрешения является преступным, когда оно:

- инкриминируется в условиях большого риска потерь, вызванных неизвестным лицом, использующим систему или наносящим вред системе или ее функционированию; или

- инкриминируется неизвестному лицу, имеющему намерение нанести ущерб и использующему для этого систему или наносящему вред системе или ее функционированию; или
- применяется в случае, когда теряется информация с помощью неизвестного автора, который использовал данную систему или нанес вред системе или
  ее функционированию.

4. Неразрешенное использование защищенной программы ЭВМ. Использование без разрешения защищенной программы ЭВМ или ее незаконное воспроизводство с намерением исправить программу таким образом, чтобы вы звать незаконную экономическую выгоду для себя или другого человека или причинить вред законному владельцу данной программы.

В последние десятилетия в США принят ряд федеральных законов, создавших правовую основу для формирования и проведения единой государственной политики в области информатизации и защиты информации. Например, Закон

Соединенных Штатов «Об обеспечении безопасности ЭВМ» № НК145, принятый конгрессом в мае 1987 г., устанавливает приоритет национальных интересов при решении вопросов безопасности информации, в том числе частной. Законом установлено, что важной является информация, «потеря которой, неправильное использование, несанкционированное изменение которой или доступ к которой могут привести к нежелательным воздействиям на национальные интересы». Установлена также новая категория информации ограниченного доступа — «несекретная, но важная с точки зрения национальной безопасности». К этой категории отнесена большая часть сведений, циркулирующих или обрабатываемых в информационно телекоммуникационных системах частных фирм и корпораций, работающих по правительственным заказам [38, с. 15].

Сегодня порядка 20 стран мира имеют национальное законодательство, относящееся к использованию глобального информационного пространства. В разряд приоритетных выдвигается вопрос о разработке правовых и организационных механизмов регулирования использования сети Интернет, где отсутствует централизованная система управления. Координатором выступает Общество участников Интернет, представляющее общественную организацию, базирующуюся на взносах участников и пожертвованиях спонсоров. Зарубежными исследователями неоднократно подчеркивалась необходимость не обременять Интернет излишним государственным регулированием. Тем не менее дальнейшее

развитие этой глобальной сети ставит ряд правовых проблем, для разрешения которых приняты и готовятся к принятию ряд законодательных актов.

1.3 Обзор технологий совершения компьютерных преступлений

По нашему мнению, следует различать компьютерную преступность как **правовую категорию и** компьютерную преступность как **социальное явление,** которое включает в себя не только совокупность всех компьютерных преступлений, но и различные формы тесно связанной с ними организационной деятельности.

При этом компьютерные преступления условно можно подразделить на две большие категории — преступления, связанные с вмешательством в работу

компьютеров, и, преступления, использующие компьютеры как необходимые технические средства.

Перечислим основные виды преступлений, связанных с вмешательством в работу компьютеров.

1. *Несанкционированный доступ к информации, хранящейся в компьютере,* который осуществляется, как правило, с использованием чужого имени, изменением физических адресов технических устройств, использованием информации, оставшейся после решения задач, модификацией программного и информационного обеспечения, хищением носителя информации, установкой аппаратуры записи, подключаемой к каналам передачи данных. При этом анализ уголовных дел показал, что в 31,8 % случаев отмечен несанкционированный доступ к информации, хранящейся на компьютере.

Хакеры, «электронные корсары», «компьютерные пираты» — так называют людей, осуществляющих несанкционированный доступ в чужие информационные сети для забавы. Набирая на удачу один номер за другим, они терпеливо дожидаются, пока на другом конце провода не отзовется чужой компьютер. После этого телефон подключается к приемнику сигналов в собственной ЭВМ, и связь установлена. Если теперь угадать код (а слова, которые служат паролем часто банальны), то можно внедриться в чужую компьютерную систему.

Несанкционированный доступ к файлам законного пользователя осуществляется также нахождением слабых мест в защите системы. Однажды обнаружив их, нарушитель может не спеша исследовать содержащуюся в системе информацию, копировать ее, возвращаться к ней неоднократно.

Программисты иногда допускают ошибки в программах, которые не удается обнаружить в процессе отладки. Авторы больших сложных программ могут не заметить некоторых слабостей логики. Уязвимые места иногда обнаруживаются и в электронных цепях. Все эти небрежности, ошибки приводят к появлению «брешей». Обычно они все-таки выявляются при проверке, редактировании, отладке программы, но абсолютно избавится от них невозможно.

Бывает, что некто проникает в компьютерную систему, выдавая себя за законного пользователя. Системы, которые не обладают средствами аутентичной идентификации (например, по физиологическим характеристикам: по отпечаткам пальцев, по рисунку сетчатки глаза, голосу и т. п.), оказываются без защиты против этого приема. Самый простейший путь его осуществления — получить коды и другие идентифицирующие шифры законных пользователей.

Это может осуществляться путем:

- приобретения (обычно подкупом персонала) списка пользователей со всей необходимой информацией;
- обнаружения такого документа в организациях, где не налажен доста-точный контроль за их хранением;
- подслушивания через телефонные линии.

Иногда случается, как например, с ошибочными телефонными звонками, что пользователь с удаленного терминала подключается к чьей-то системе, будучи абсолютно уверенным, что он работает с той системой, с какой и намеревался. Владелец системы, к которой произошло фактическое подключение, формируя правдоподобные отклики, может поддерживать это заблуждение в течение определенного времени и таким образом получить некоторую информацию, в частности коды.

В любом компьютерном центре имеется особая программа, применяемая как системный инструмент в случае возникновения сбоев или других отклонений в работе ЭВМ, своеобразный аналог приспособлений, помещаемых в транспорте под надписью «разбить стекло в случае аварии». Такая программа — мощный и опасный инструмент в руках злоумышленника.

Несанкционированный доступ может осуществляться в результате системной поломки. Например, если некоторые файлы пользователя остаются открытыми, он может получить доступ к непринадлежащим ему частям банка данных. Все происходит так словно клиент банка, войдя в выделенную ему в хранилище комнату, замечает, что там нет одной стены. В таком случае он может проникнуть в чужие сейфы и похитить все, что в них хранится.

2. *Ввод в програлинное обеспечение «логических бомб»,* которые срабатывают при выполнении определенных условий и частично или полностью выводят из строя компьютерную систему.

«Временная бомба» является разновидностью «логической бомбы», которая срабатывает по достижении определенного момента времени [24].

Способ «троянский конь» состоит в тайном введении в чужую программу таких команд, которые позволяют осуществлять новые, не планировавшиеся владельцем программы функции, но одновременно сохранять и прежнюю работоспособность.

С помощью «троянского коня» преступники, например, отчисляют на свой счет определенную сумму с каждой операции.

Компьютерные программные тексты обычно чрезвычайно сложны. Они состоят из сотен, тысяч, а иногда и миллионов команд. Поэтому «троянский конь» из нескольких десятков команд вряд ли может быть обнаружен, если, конечно, нет подозрений относительно того, что он может появиться. Но и в последнем случае экспертам-программистам потребуется достаточно времени, чтобы найти его.

Есть еще одна разновидность «троянского коня». Ее особенность состоит в том, что в безобидно выглядевшем куске программы вставляются не команды, собственно, выполняющие «грязную» работу, а команды, формирующие эти команды и после выполнения уничтожающие их. В этом случае программисту, пытающемуся найти «троянского коня», необходимо искать не его самого, а команды, его формирующие. Развивая эту идею, можно представить себе команды, которые создают команды и т. д. (сколь угодно большое число раз), создающие «троянского коня».

В США получила распространение форма компьютерного вандализма, при которой «троянский конь» разрушает через какой-то промежуток времени все программы, хранящиеся в памяти машины. Во многих поступивших в продажу компьютерах оказалась «временная бомба», которая «взрывается» в самый неожиданный

момент, разрушая всю библиотеку данных [24]. Не следует думать, что «логические бомбы» — это экзотика, несвойственная нашему обществу.

3. *Разработка и распространение компьютерных вирусов.*

«Троянский конь» типа «сотри все данные этой программы, перейди в следующую и сделай то же самое» обладает свойствами переходить через коммуникационные сети из одной системы в другую, распространяясь как вирусное заболевание.

Выявляется вирус не сразу: первое время компьютер «вынашивает инфекцию», поскольку для маскировки вирус нередко используется в комбинации с «логической бомбой» или «временной бомбой». Вирус наблюдает за всей обрабатываемой информацией и может перемещаться, используя пересылку этой информации. Все происходит, как если бы он заразил белое кровяное тельце и путешествовал с ним по организму человека.

Начиная действовать (перехватывать управление), вирус дает команду компьютеру, чтобы тот записал зараженную версию программы. После этого он возвращает программе управление. Пользователь ничего не заметит, так как его компьютер находится в состоянии «здорового носителя вируса». Обнаружить этот вирус можно, только обладая чрезвычайно развитой программистской интуицией, поскольку никакие нарушения в работе ЭВМ в данный момент не проявляют *себя.* А в один прекрасный день компьютер «заболевает».

По оценке специалистов в «обращении» находится более 100 типов вирусов. Их можно разделить на две разновидности — «вульгарный вирус» и «раздробленный вирус». Вирусы могут быть внедрены в операционную систему, прикладную программу или в сетевой драйвер. Варианты вирусов зависят от целей, преследуемых их создателем. Признаки их могут быть относительно доброкачественными, например, замедление в выполнении программ или появление светящейся точки на экране дисплея (так называемый «итальянский попрыгунчик»). Признаки могут быть эволютивными, и «болезнь» будет обостряться по мере своего течения. Так, по непонятным причинам программы начинают переполнять магнитные диски, в результате чего существенно увеличивается объем программных файлов. Наконец, эти проявления могут быть катастрофическими и привести к стиранию файлов и уничтожению программного обеспечения [7].

В печати часто проводится параллель между компьютерным вирусом и вирусом «AIDS». Только упорядоченная жизнь с одним или несколькими партнерами

способна уберечь от этого вируса. Беспорядочные связи со многими компьютерами почти наверняка приводят к заражению. Естественно, что против вирусов были приняты чрезвычайные меры, приведшие к созданию текстовых программ-антивирусов. Защитные программы подразделяются на три вида: фильтрующие (препятствующие проникновению вируса), противоинфекцион-ные (постоянно контролирующие процессы в системе) и противовирусные (настроенные на выявление отдельных вирусов). Однако развитие этих программ пока не успевает за развитием компьютерной эпидемии.

Заметим, что пожелание ограничить использование непроверенного программного обеспечения скорее всего так и останется практически невыполнимым. Это связано с тем, что фирменные программы на «стерильных» носителях стоят немалых денег. Поэтому избежать их неконтролируемого копирования почти невозможно.

Следует отметить, что распространение компьютерных вирусов имеет и некоторые положительные стороны. В частности, они являются, по-видимому, лучшей защитой от похитителей программного обеспечения. Зачастую разработчики сознательно заражают свои дискеты каким-либо безобидным вирусом, который хорошо обнаруживается любым антивирусным тестом. Это служит достаточно надежной гарантией, что никто не рискнет копировать такую дискету. И кроме того, анализ уголовных дел показал, что в 54,7 % случаев привлекались к уголовной ответственности именно за создание, использование и распространение вредоносных программ.

4. *Преступная небрежность в разработке, изготовлении и эксплуата-ции программно-вычислительных комплексов, приведшая к тяжким по следствиям.*

Проблема неосторожности в области компьютерной техники сродни неосторожной вине при использовании любого другого вида техники, транспорта и т. п. Особенностью компьютерной неосторожности является то, что безошибочных программ в принципе не бывает. Если проект практически в любой области техники можно выполнить с огромным запасом надежности, то в области программирования такая надежность весьма условна, а в ряде случаев почти не достижима.

5. *Подделка компьютерной информации.*

По-видимому, этот вид компьютерной преступности является одним из наиболее «свежих». Он является разновидностью несанкционированного доступа с той

разницей, что пользоваться им может, как правило, не посторонний пользователь, а сам разработчик, причем имеющий достаточно высокую квалификацию.

Идея преступления состоит в подделке выходной информации компьютеров с целью имитации работоспособности больших систем, составной частью которых является компьютер. При достаточно ловко выполненной подделке зачастую удается сдать заказчику заведомо неисправную продукцию.

К подделке информации можно отнести также подтасовку результатов выборов, голосований, референдумов и т. п. Ведь если каждый голосующий не может убедиться, что его голос зарегистрирован правильно, то всегда возможно внесение искажений в итоговые протоколы.

Естественно, что подделка информации может преследовать и другие цели.

6. *Хищение компьютерной информации.*

Если «обычные» хищения подпадают под действие существующего уголовного закона, то проблема хищения информации значительно более сложна. Присвоение машинной информации, в том числе программного обеспечения, путем несанкционированного копирования не квалифицируется как хищение, поскольку хищение сопряжено с изъятием ценностей из фондов организации. Не очень далеко от истины то, что у нас программное обеспечение распространяется только путем краж и обмена краденым. При неправомерном обращении в собственность машинная информация может не изыматься из фондов, а копироваться. Следовательно, как уже отмечалось выше, машинная информация должна быть выделена как самостоятельный предмет уголовно-правовой охраны. Собственность на информацию, как и прежде, не закреплена в законодательном порядке. На наш взгляд, последствия этого не замедлят сказаться. Тем более, что анализ уголовных дел выявил 4,7 % случаев незаконного присвоения компьютерной информации, а остальные 8,8 % относятся к различного рода компьютерным преступлениям, которые относятся ко второй категории преступлений.

Рассмотрим теперь **вторую категорию преступлений, в которых компьютер является средством достижения цели.** Здесь можно выделить разработку сложных математических моделей, входными данными в которых являются возможные условия проведения преступления, а выходными — рекомендации по выбору оптимального варианта действий преступника.

Другой вид преступлений с использованием компьютеров получил название *«воздушный змей».*

В простейшем случае требуется открыть в двух банках по небольшому счету. Далее деньги переводятся из одного банка в другой и обратно с постепенно повышающимися суммами. Хитрость заключается в том, чтобы до того, как в банке обнаружится, что поручение о переводе не обеспечено необходимой суммой, приходило бы извещение о переводе в этот банк, так чтобы общая сумма покрывала требование о первом переводе. Этот цикл повторяется большое число раз («воздушный змей» поднимается все выше и выше) до тех пор, пока на счете не оказывается приличная сумма (фактически она постоянно «перескакивает» с одного счета на другой, увеличивая свои размеры). Тогда деньги быстро снимаются, а владелец счета исчезает. Этот способ требует очень точного расчета, но для двух банков его можно сделать и без компьютера. На практике в такую игру включают большое количество банков: так сумма накапливается быстрее и число поручений о переводе не достигает подозрительной частоты. Но управлять этим процессом можно только с помощью компьютера.

Можно представить *cqGq* создание специализированного компьютера-шпиона, который будучи подключен к разведуемой сети, генерирует всевозможные запросы, фиксирует и анализирует полученные ответы. Поставить преграду перед таким хакером практически невозможно. Поэтому нетрудно предположить, что организованная преступность давно приняла на вооружение технику, которая не только является предметом преступления, но и средством достижения поставленных целей.

Глава 2. Технологии предупреждения компью-терных преступлений

2.1 Меры защиты данных

Рассмотрим некоторые из мер, направленных на предупреждение компьютерных преступлений.

1. Защита данных в компьютерных сетях.

При рассмотрении проблем защиты данных в сети прежде всего возникает вопрос о классификации сбоев и нарушений прав доступа, которые могут привести к уничтожению или нежелательной модификации данных. Среди таких потенциальных «угроз» можно выделить:

1. Сбои оборудования: кабельной системы; электропитания; дисковых систем; систем архивации данных; работы серверов, рабочих станций, сетевых карт и т. д.

2. Потери информации из-за некорректной работы ПО:

-потеря или изменение данных при ошибках ПО;

-потери при заражении системы компьютерными вирусами.

3. Потери, связанные с несанкционированным доступом:

несанкционированное копирование, уничтожение или подделка информации;

ознакомление с конфиденциальной информацией, составляющей тайну, посторонних лиц.

1. Потери информации, связанные с неправильным хранением архивных данных.
2. Ошибки обслуживающего персонала и пользователей:

-случайное уничтожение или изменение данных;

-некорректное использование программного и аппаратного обеспечения, ведущее к уничтожению или изменению данных.

В зависимости от возможных видов нарушений работы сети (под нарушением работы, на наш взгляд, необходимо понимать и несанкционированный доступ) многочисленные виды защиты информации объединяются в три основных класса:

-средства физической защиты, включающие средства защиты кабельной системы, систем электропитания, средства архивации, дисковые массивы и т.д.;

-программные средства защиты, в том числе антивирусные программы, системы разграничения полномочий, программные средства контроля доступа;

-административные меры защиты, включающие контроль доступа в помещения, разработку стратегии безопасности фирмы, планов действий в чрезвычайных

ситуациях и т. д.

Следует отметить, что подобное деление достаточно условно, поскольку современные технологии развиваются в направлении сочетания программных и аппаратных средств защиты. Наибольшее распространение такие программно-аппаратные средства получили, в частности, в области контроля доступа, защиты от вирусов и т. д.

Концентрация информации в компьютерах (аналогично концентрации наличных денег в банках) заставляет все более усиливать контроль в целях защиты информации. Юридические вопросы, частная тайна, национальная безопасность — все эти соображения требуют усиления внутреннего контроля в коммерческих и правительственных организациях. Работы в этом направлении привели к появлению новой дисциплины — безопасность информации. Специалист в области безопасности информации отвечает за разработку, реализацию и эксплуатацию системы обеспечения информационной безопасности, направленной на поддержание целостности, пригодности и конфиденциальности накопленной в организации информации. В его функции входит обеспечение физической (технические средства, линии связи и удаленные компьютеры) и логической (данные, прикладные программы, операционная система) защиты информационных ресурсов.

Сложность создания системы защиты информации определяется тем, что данные могут быть похищены из компьютера и одновременно оставаться на месте; ценность некоторых данных заключается в обладании ими, а не в уничтожении или изменении.

Обеспечение безопасности информации — дорогое дело, и не столько из-за затрат на закупку или установку средств, сколько из-за того, что трудно квалифицированно определить границы разумной безопасности и соответствующего поддержания системы в работоспособном состоянии.

Если локальная сеть разрабатывалась в целях совместного использования лицензионных программных средств, дорогих цветных принтеров или больших файлов общедоступной информации, то нет никакой потребности даже в минимальных системах шифрования/дешифрования информации.

Средства защиты информации нельзя проектировать, покупать или устанавливать до тех пор, пока не произведен соответствующий анализ риска, который должен дать объективную оценку многих факторов (подверженность появлению

нарушения работы, вероятность появления нарушения работы, ущерб от коммерческих потерь, снижение коэффициента готовности системы, общественные отношения, юридические проблемы) и предоставить информацию для определения подходящих типов и уровней безопасности. Коммерческие организации все в большей степени переносят критическую корпоративную информацию с больших вычислительных систем в среду открытых систем и встречаются с новыми и сложными проблемами при реализации и эксплуатации системы безопасности. Сегодня все больше организаций разворачивают мощные распределенные базы данных и приложения «клиент/сервер» для управления коммерческими данными. При увеличении распределения возрастает также и риск неавторизованного доступа к данным и их искажения [7].

Шифрование данных традиционно использовалось правительственными и оборонными департаментами, но в связи с изменением потребностей и некоторые наиболее солидные компании начинают использовать возможности, предоставляемые шифрованием для обеспечения конфиденциальности информации.

Финансовые службы компаний (прежде всего в США) представляют важную и большую пользовательскую базу и часто специфические требования предъявляются к алгоритму, используемому в процессе шифрования. Опубликованные алгоритмы, например DES, являются обязательными. В то же время, рынок коммерческих систем не всегда требует такой строгой защиты, как правительственные или оборонные ведомства, поэтому возможно применение продуктов и другого типа, например, PGP (Pretty Good Privacy).

2. Шифрование.

Шифрование данных может осуществляться в режимах On-line (в темпе поступления информации) и Off-line (автономном). Остановимся подробнее на первом типе, представляющем большой интерес. Наиболее распространены два алгоритма.

Стандарт шифрования данных DES (Data Encryption Standart) был разработан фирмой IBM в начале 70-х годов и в настоящее время является правительственным стандартом для шифрования цифровой информации. Он рекомендован Ассоциацией Американских Банкиров. Сложный алгоритм DES использует ключ длиной *56* бит и 8 битов проверки на четность и требует от злоумышленника перебора 72 квадрилионов возможных ключевых комбинаций, обеспечивая высокую степень защиты при небольших расходах. При частой смене ключей

алгоритм удовлетворительно решает проблему превращения конфиденциальной информации в недоступную.

Алгоритм RSA был изобретен Ривестом, Шамиром и Альдеманом в 1976 г. и представляет собой значительный шаг в криптографии. Этот алгоритм также был принят в качестве стандарта Национальным Бюро Стандартов.

DES технически является симметричным алгоритмом, а RSA — асимметричным, то есть он использует разные ключи при шифровании и дешифровании. Пользователи имеют два ключа и могут широко распространять свой открытый ключ. Открытый ключ используется для шифрования сообщения пользователем, но только определенный получатель может дешифровать его своим секретным ключом; открытый ключ бесполезен для дешифрования. Это делает ненужными секретные соглашения о передаче ключей между корреспондентами. DES определяет длину данных и ключа в битах, а RSA может быть реализован при любой длине ключа. Чем длиннее ключ, тем выше уровень безопасности (но становится длительнее и процесс шифрования и дешифрования). Если ключи DES можно сгенерировать за микросекунды, то примерное время генерации ключа RSA — десятки секунд. Поэтому открытые ключи RSA предпочитают разработчики программных средств, а секретные ключи DES — разработчики аппаратуры [8].

3. Физическая защита данных.

Кабельная *система* остается главной «ахилессовой пятой» большинства локальных вычислительных сетей: по данным различных исследований, именно кабельная система является причиной более чем половины всех отказов сети. В связи с этим кабельной системе должно уделяться особое внимание с самого момента проектирования сети.

Наилучшим образом избавить себя от «головной боли» по поводу неправильной прокладки кабеля является использование получивших широкое распространение в последнее время так называемых структурированных кабельных систем, использующих одинаковые кабели для передачи данных в локальной вычислительной сети, локальной телефонной сети, передачи видеоинформации или сигналов от датчиков пожарной безопасности или охранных систем. К структурированным кабельным системам относятся, например, «SYSTIMAX SCS» фирмы «AT&T», «OPEN DECconnect» компании «Digital», кабельная система корпорации ЮМ.

Понятие «структурированность» означает, что кабельную систему здания можно разделить на несколько уровней в зависимости от назначения и место расположения ее компонентов. Например, кабельная система «SYSTIMAX SCS» состоит из:

внешней подсистемы (campus subsystem);

аппаратных (equipment room);

административной подсистемы (administrative subsystem);

магистрали (backbone cabling);

горизонтальной подсистемы (horizontal subsystem);

рабочих мест (work location subsystem) [9].

Внешняя подсистема состоит из медного оптоволоконного кабеля, устройств электрической защиты и заземления и связывает коммуникационную и обрабатывающую аппаратуру в здании (или комплексе зданий). Кроме того, в эту подсистему входят устройства сопряжения внешних кабельных линий и внутренних.

Аппаратные служат для размещения различного коммуникационного оборудования, предназначенного для обеспечения работы административной подсистемы.

Административная подсистема предназначена для быстрого и легкого управления кабельной системы «SYSTIMAX SCS» при изменении планов размещения персонала и отделов. В ее состав входят кабельная система (неэкрани-рованная витая пара и оптоволокно), устройства коммутации и сопряжения магистрали и горизонтальной подсистемы, соединительные шнуры, маркировочные средства и т. д.

Магистраль состоит из медного кабеля или комбинации медного и оптоволоконного кабеля и вспомогательного оборудования. Она связывает между собой этажи здания или большие площади одного и того же этажа.

Горизонтальная система на базе витого медного кабеля расширяет основную магистраль от входных точек административной системы этажа к розеткам на рабочем месте. И, наконец, оборудование рабочих мест включает в себя соединительные шнуры, адаптеры, устройства сопряжения и обеспечивает

механическое и электрическое соединение между оборудованием рабочего места и горизонтальной кабельной подсистемы.

Системы электроснабжения. Наиболее надежным средством предотвращения потерь информации при кратковременном отключении электроэнергии в настоящее время является установка источников бесперебойного питания. Подобные устройства, различные по своим техническим и потребительским характеристикам, могут обеспечить питание всей локальной сети или отдельной компьютера в течение промежутка времени, достаточного для восстановления подачи напряжения или для сохранения информации на магнитные носители. Большинство источников бесперебойного питания одновременно выполняет функции и стабилизатора напряжения, что является дополнительной защитой **от** скачков напряжения в сети. Многие современные сетевые устройства (серверы, концентраторы, мосты и т. д.) оснащены собственными дублированными системами электропитания.

За рубежом корпорации имеют собственные аварийные электрогенераторы или резервные линии электропитания. Эти линии подключены к разным подстанциям, и при выходе из строя одной из них электроснабжение осуществляется с резервной подстанции.

Системы архивирования и дублирования информации.

Организация надежной и эффективной системы архивации данных является одной из важнейших задач по обеспечению сохранности информации в сети. В небольших сетях, где установлены один-два сервера, чаще всего применяется установка системы архивации непосредственно в свободные слоты серверов. В крупных корпоративных сетях наиболее предпочтительно организовать выделенный специализированный архивационный сервер.

Хранение архивной информации, представляющей особую ценность, должно быть организовано в специальном охраняемом помещении. Специалисты рекомендуют хранить дубликаты архивов наиболее ценных данных в другом здании, на случай пожара или стихийного бедствия.

4. Защита от стихийных бедствий.

Основной и наиболее распространенный метод защиты информации и оборудования от различных стихийных бедствий (пожаров, землетрясений, наводнений и т. д.) состоит в хранении архивных копий информации или в размещении

некоторых сетевых устройств, например, серверов баз данных, в специальных защищенных помещениях, расположенных, как правило, в других зданиях или, реже, даже в другом районе города или в другом городе.

2.2 Программные и программно-аппаратные методы защиты

Защита от компьютерных вирусов.

Вряд ли найдется хотя бы один пользователь или администратор сети, который бы ни разу не сталкивался с компьютерными вирусами. По данным исследования, проведенного фирмой «Creative Strategies Research», 64 % из 451 опрошенного специалиста испытали «на *севе*» действие вирусов. Сегодня дополнительно к тысячам уже известных вирусов ежемесячно появляется 100-150 новых штаммов. Наиболее распространенными методами защиты от вирусов по сей день остаются различные антивирусные программы.

Однако в качестве перспективного подхода к защите от компьютерных вирусов в последние годы все чаще применяется сочетание программных и аппаратных методов защиты. Среди аппаратных устройств такого плана можно отметить специальные антивирусные платы, которые вставляются в стандартные слоты расширения компьютера. Корпорация Intel в 1994 г. предложила перспективную технологию защиты от вирусов в компьютерных сетях. Flash-память сетевых адаптеров Intel EtherExpress PRO/10 содержит антивирусную программу, сканирующую все системы компьютера еще до его загрузки.

Защита от несанкционированного доступа.

Проблема защиты информации от несанкционированного доступа особо обострилась с широким распространением локальных и, особенно, глобальных компьютерных сетей. Необходимо также отметить, что зачастую ущерб наносится не из-за «злого умысла», а из-за элементарных ошибок пользователей, которые случайно портят или удаляют жизненно важные данные. В связи с этим, помимо контроля доступа, необходимым элементом защиты информации в компьютерных сетях является разграничение полномочий пользователей.

В компьютерных сетях при организации контроля доступа и разграничения полномочий пользователей чаще всего используются встроенные средства сетевых

операционных систем. Так, крупнейший производитель сетевых ОС — корпорация «Novell» в своем последнем продукте «NetWare 4.1» предусмотрел помимо стандартных средств ограничения доступа, таких, как система паролей и разграничения полномочий, ряд новых возможностей, обеспечивающих первый класс защиты данных. Новая версия «NetWare» предусматривает, в частности, возможность кодирования данных по принципу «открытого ключа» (алгоритм RSA) с формированием электронной подписи для передаваемых по сети пакетов.

В такой системе организации защиты все равно остается слабое место: уровень доступа и возможность входа в систему определяются паролем. Не секрет, что пароль можно подсмотреть или подобрать. Для исключения возможности неавторизованного входа в компьютерную сеть в последнее время используется комбинированный подход — пароль + идентификация пользователя по персональному «ключу». В качестве «ключа» может использоваться пластиковая карта (магнитная или со встроенной микросхемой «smart-card») или различные устройства для идентификации личности по биометрической информации — по радужной оболочке глаза или отпечаткам пальцев, размерам кисти руки и так далее.

Оснастив сервер или сетевые рабочие станции, например, устройством чтения смарт-карточек и специальным программным обеспечением, можно значительно повысить степень защиты от несанкционированного доступа. В этом случае для доступа к компьютеру пользователь должен вставить смарт-карту в устройство чтения и ввести свой персональный код. Программное обеспечение позволяет установить несколько уровней безопасности, которые управляются системным администратором. Возможен и комбинированный подход с вводом дополнительного пароля, при этом приняты специальные меры против «перехвата» пароля с клавиатуры. Этот подход значительно надежнее применения паролей, поскольку, если пароль подглядели, пользователь об этом может не знать, если же пропала карточка, можно принять меры немедленно.

Смарт-карты управления доступом позволяют реализовать, в частности, такие функции, как контроль входа, доступ к устройствам персонального компьютера, к программам, файлам и командам. Кроме того, возможно также осуществление контрольных функций, в частности, регистрация попыток нарушения доступа к ресурсам, использования запрещенных утилит, программ, команд DOS.

Одним из удачных примеров создания комплексного решения контроля доступа в открытых системах, основанного на программных и на аппаратных средствах

защиты, стала система «Kerberos», в основе которой лежат три компонента:

1) база данных,

2) авторизационный сервер,

3) сервер выдачи разрешений.

Защита информации при удаленном доступе.

По мере расширения деятельности предприятий, роста численности персонала и появления новых филиалов возникает необходимость доступа удаленных пользователей (или групп пользователей) к вычислительным и информационным ресурсам главного офиса компании. Чаще всего для организации удаленного доступа используются кабельные линии (обычные телефонные или выделенные) и радиоканалы. В связи с этим защита информации, передаваемой по каналам удаленного доступа, требует особого подхода.

В частности, в мостах и маршрутизаторах удаленного доступа применяется сегментация пакетов — их разделение и передача параллельно по двум линиям, что делает невозможным «перехват» данных при незаконном подключении «хакера» к одной из линий. К тому же используемая при передаче данных процедура сжатия передаваемых пакетов гарантирует невозможности расшифровки «перехваченных» данных. Кроме того, мосты и маршрутизаторы удаленного доступа могут быть запрограммированы таким образом, что удаленные пользователи будут ограничены в доступе к отдельным ресурсам сети главного офиса.

Разработаны и специальные устройства контроля доступа к компьютерным сетям по коммутируемым линиям. Например, фирмой «AT&T» предлагается модуль «Remote Port Security Device» (PRSD), представляющий собой два блока размером с обычный модем: «RPSD Lock» (замок), устанавливаемый в центральном офисе, и «RPSD Key» (ключ), подключаемый к модему удаленного пользователя. RPSD Key и Lock позволяют установить несколько уровней защиты и контроля доступа, в частности:

шифрование данных, передаваемых по линии при помощи генерируемых цифровых ключей;

контроль доступа в зависимости от дня недели или времени суток (всего 14 ограничений) [10].

Широкое распространение радиосетей в последние годы поставило разработчиков радиосистем перед необходимостью защиты информации от «хакеров», вооруженных разнообразными сканирующими устройствами. Были применены разнообразные технические решения. Например, в радиосети компании «RAM Mobil Data» информационные пакеты передаются через разные каналы и базовые станции, что делает практически невозможным для посторонних собрать всю передаваемую информацию воедино. Активно используются в радио сетях и технологии шифрования данных при помощи алгоритмов DES и RSA.

Таким образом, мы попытались обосновать лишь некоторые соображения, связанные с профилактикой и предупреждением компьютерной преступности, которые требуют комплексного подхода с учетом основных объективных и субъективных причин и условий, способствующих совершению компьютерных преступлений, к которым в большинстве случаев относятся:

1) неконтролируемый доступ к компьютеру, используемого как автономно, так и в качестве дистанционной передачи данных в процессе осуществления определенных операций (например, финансовых);

2) бесконтрольность за действиями обслуживающего персонала, что позволяет преступнику свободно использовать ЭВМ в качестве орудия совершения преступления;

3) низкий уровень программного обеспечения, не имеющего соответствующей защиты информации;

4) несовершенство парольной системы защиты от несанкционированного доступа к программному обеспечению;

5) отсутствие лица, отвечающего за конфиденциальность коммерческой информации и ее безопасность в части защиты средств компьютерной техники от несанкционированного доступа;

6) отсутствие письменных договоров на предмет неразглашения коммерческой и служебной тайны, персональных данных и иной конфиденциальной информации;

Заключение

Подводя итоги исследования, считаем необходимым сформулировать определенные выводы и предложения, реализация которых будет способствовать повышению эффективности борьбы с компьютерной преступностью.

Компьютерная преступность представляет собой естественный и необходимый результат эволюции общества, основанный на информационных технологиях, выступает как дополнительная комфортная форма жизнедеятельности человека, не поддающаяся ликвидации либо преодолению и требующая адекватных способов и методов регулирования и управления в целях минимизации причиняемого вреда интересам личности, общества и государства, обладающая признаками профессиональной преступности и представляющая собой виновное нарушение уголовно-правовых запретов и совокупность всех фактически совершенных преступлений в сфере информационных технологий.

Таким образом, доступ к компьютерной информации — это санкционированное собственником (владельцем) информации ознакомление лица со сведениями, содержащимися на машинном носителе, в ЭВМ, системе ЭВМ или их сети. В свою очередь несанкционированное ознакомление означает, что у лица нет права на такие действия (это показывает на неправомерность доступа).

Неправомерный доступ — проникновение, совершенное путем: использования специальных технических или программных средств, позволяющих преодолеть установленные системы защиты; незаконного использования действующих паролей или кодов для проникновения в компьютер, совершения иных действий в целях проникновения в систему или сеть под видом законного пользователя; хищения носителей информации, при условии, что были приняты меры их охраны, если это деяние повлекло уничтожение или блокирование информации, которые в свою очередь всегда сопровождаются совершением активных действий неправомерного характера (модификация, копирование и иные нарушения работы ЭВМ).

Под охраняемой законом информацией понимается информация, для которой в специальных законах установлен специальный режим ее правовой защиты. Например, к ней можно отнести государственные секреты, положения закона о национальной системе защиты информации и государственных информационных ресурсов, служебную тайну и т. д.

Анализ научной и специальной литературы показывает, что компьютерные преступления в современных условиях имеют тенденцию к росту. Около 500

компьютерных посягательств на информационные сети государственных органов Казахстана происходит ежемесячно. Электронные взломщики регулярно пытаются взломать базы данных банков и коммерческих предприятий, чтобы снять крупные суммы денег или получить конфиденциальную информацию. Проблема компьютерной преступности как негативного социального явления в последнее время приобрела международную значимость из-за транснационального характера. В рамках Протокола о сотрудничестве в области борьбы с преступлениями в сфере компьютерной информации с участием спецслужб государств-участников СНГ имеется определенный практический опыт. Одним из приоритетных вопросов в данной области является развитие сотрудничества с европейскими и западными странами.

Список использованной литературы

1. ВеховВ. Б. Компьютерные преступления: способы совершения, методы расследования. — М., 2018. — 296 с.
2. Правовая информатика и кибернетика: Учебник для ВУЗов / Под ред. Н. С. Полевого. —- М., 2019. — 527 с.
3. Скоромников К. С. Неправомерный доступ к компьютерной информации и его расследование // Прокурорский надзор и следственная практика. —2017.— №1. — С. 165-169.
4. Комментарий к Уголовному кодекса РФ / Отв. ред. д-р юрид. наук, проф. А. В. Наумов. —М., 2019. — 876 с.
5. Смирнова Т. Г. Уголовно-правовая борьба с преступлениями в сфере компьютерной информации: автореф. дис. ... канд. юрид. наук. — М., 1998. —24 с.
6. Добровольский Д. В. Актуальные проблемы борьбы с компьютерной преступностью: дис. канд. юрид. наук. — М., 2006. — 225 с.
7. Более 30 тысяч сайтов обучают компьютерному взлому // www/cnews/ru.
8. Реальные преступления в виртуальном мире // Жизненное пространство. — 2015. — № 12. — С. 21-23.
9. Баранов А. П., Фатьянов А. А. Организационно-технические меры борьбы с компьютерной преступностью. Проблемы сертификации и лицензирования // Вестник Российского общества информатики и вычислительной техники — 2017. — № 4. — С. 32-33.
10. Вязанцев В. Последние достижения мирового хакерства // Свободный курс. — 2009. — № 16. — С. 13-15.

11. Кокоткин А. Компьютерные взломщики // Аргументы и факты. 2018. 8 апреля.
12. Хакеры атакуют американскую систему обороны // Конфидент. — 1920. — №3. —С. 8-9.