Содержание:

Введение

Благодаря научно - технической революции появился новый вид общественных отношений и общественных ресурсов — информационных. Которые в целом отличаются от сырьевых, энергетических ресурсов целым рядом особенностей. Информация превратилась в продукт общественных т.е. информационных отношений, начинала завоевывать товарные черты и стала предметом купли - продажи. Появилось множество проблем, сопутствующих новым технологиям.

Жизнь современного человека сложно представить без компьютерных технологий, которые, в настоящее время, присутствуют практически во всех сферах жизни общества. Данный факт привел к тому, что появилось так называемое «информационное общество» - общество нового типа. Но в то же время, чем более компьютеризированным становится наше общество, тем выше риск совершения преступлений с использованием глобальных информационно - телекоммуникационных систем и сетей. Преступники быстрее осваивают новые технологии, опережая законодательство и правоприменителей.

Глобальная компьютеризация привела к тому, что число компьютерных преступлений, а, следовательно, экономический ущерб от их совершения, ежегодно растет[1]. Сегодня компьютерная преступность - один из самых опасных видов преступных посягательств.

Объектом исследования в курсовой работе являются компьютерные преступления.

Предмет исследования – технологии совершения компьютерных преступлений.

Целью исследования в курсовой работе является углубленный анализ используемых технологий совершения компьютерных преступлений.

Для достижения поставленной цели сформулированы следующие задачи:

1. изучить сущность понятия «компьютерные преступления»;
2. рассмотреть классификацию компьютерных преступлений;
3. проанализировать технологии совершения компьютерных преступлений.

Методической основой курсовой работы являются учебная и методическая литература, статьи в периодической печати и Интернет-ресурсы.

Глава 1. Теоретические основы совершения компьютерных преступлений

Сущность понятия «компьютерные преступления»

Понятие «компьютерные преступления» впервые возникло в иностранной литературе в начале 60-х гг. XX в[2]. С распространением информационных технологий в повседневной жизни вследствие повышения количества преступных посягательств, совершенных с применением электронно-вычислительной техники, эта дефиниция получила широкое применение[3].

В российской уголовно-правовой науке отсутствует ясное определение понятия компьютерного преступления. Уголовный Кодекс РФ фиксирует лишь составы преступлений, то есть перечень признаков, описывающих преступление как общественно опасное деяние, таким образом, перечисляя те виды действий, которые совершаются в отношении компьютерной информации и которые можно относить к преступлениям, посягающим на безопасность компьютерной информации. На интернациональном уровне также часто обращалось внимание на невозможность дать полное определение компьютерного преступления.

Получивший широкое практическое применение в начале 90-х гг. термин computer crimes, был впервые использован в докладе Стэндфордского исследовательского института еще в конце 70-х гг. прошлого столетия. Состав же компьютерных преступлений был сформулирован в 1979 году на конференции Американской ассоциации адвокатов в Далласе. Первая попытка разработки понятия компьютерного преступления была предпринята в 1983 году в рамках Организации экономического сотрудничества и развития (ОЭСР). Целью ОЭСР было обсуждение возможности международной гармонизации уголовного законодательства отдельных государств для борьбы с экономическими компьютерными преступлениями. Комитетом был предложен единый список деяний, которые должны рассматриваться как компьютерные преступления в законодательстве государств-членов[4].

В настоящее время в отечественной юридической науке существует несколько мнений различных групп ученых по поводу того, что следует понимать под данным термином.

Сторонники первого направления, в частности, Ю. М. Батурин и А. М. Жодзишский, считают, что «компьютерных преступлений, как преступлений специфических в юридическом смысле, не существует» [5]. Правильнее говорить о компьютерных аспектах преступлений. Один из основных аргументов в пользу такой точки зрения: преступления не принято дифференцировать по видам технических средств, с помощью которых они совершаются. Эта позиция определила бурную дискуссию о криминализации преступных деяний в компьютерной сфере при принятии нового Уголовного кодекса в 1996 г. И сейчас встречаются мнения об ошибочности включения в УК РФ гл. 28 «Преступления в сфере компьютерной информации»[6].

Вторая группа ученых (В. Б. Вехов[7], Ю. И. Ляпунов[8], В. Ю. Максимов, Н. А. Селиванов[9] и др.) полагают, что поскольку данный термин прочно вошел в международную профессиональную лексику, такая формулировка имеет право на существование. При этом ученые отмечают, что хотя понятие «компьютерные преступления» нельзя использовать строго в уголовно -правовом значении, однако его употребление целесообразно в криминологическом и криминалистическом аспектах, то есть когда речь идет о личности преступника или способе совершения преступления[10].

Сторонники третьей позиции (В. А. Копылов[11], В. В. Крылов[12], В. А. Пархомов[13] и др.) предлагают рассматривать компьютерные преступления как часть более общей группы — информационных преступлений. При этом отмечается, что каждое пятое предусмотренное Уголовным кодексом РФ преступное деяние по своей сути является информационным, то есть имеет общий объект — отношения в информационной сфере, а объективная сторона таких преступлений заключается либо в распространении (предоставлении) запрещенной или заведомо ложной информации, либо в непредставлении сведений.

Российский законодатель отказался от понятия «компьютерные преступления», введя в Уголовный кодекс 1996 г. гл. 28 «Преступления в сфере компьютерной информации». При этом был применен традиционный подход отграничения деяний от смежных составов по объекту преступных посягательств. Главным признаком данной категории преступлений выступает не компьютер, используемый в качестве орудия преступления. Таковыми являются информационные отношения,

складывающиеся в процессе создания, обработки, накопления, хранения, поиска, распространения и предоставления потребителю компьютерной информации, а также создания и использования информационных технологий, средств их обеспечения и, главным образом, защиты охраняемой законом компьютерной информации.

Глава 28 помещена в раздел IX «Преступления против общественной безопасности и общественного порядка» и включает в себя три статьи: 272 (Неправомерный доступ к компьютерной информации), 273 (Создание, использование и распространение вредоносных компьютерных программ), 274 (Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей).

Наименование «преступления в сфере компьютерной информации» вошло как в лексику науки уголовного права, так и в лексику международных правовых документов, например, в Соглашении о сотрудничестве государств-участников СНГ в борьбе с преступлениями в сфере компьютерной информации. В данном документе дается следующее определение: «Преступление в сфере компьютерной информации — уголовно наказуемое деяние, предметом которого является компьютерная информация»[14]. Представляется, что термин в том смысле, в котором он используется в Соглашении, является неоправданно узким.

Следует отметить, что теория и практика до настоящего времени не выработали единого определения понятия преступлений в сфере компьютерной информации.

Так, В. С Комиссаров предлагает «преступлениями в сфере компьютерной информации» признавать «умышленные общественно опасные деяния (действие или бездействие), причиняющие вред либо создающие угрозу причинения вреда общественным отношениям, регламентирующим безопасное производство, хранение, использование или распространение информации и информационных ресурсов либо их защиту»[15]. Представляется, что определение, предложенное Б. С. Комиссаровым, является более точным, поскольку содержит указание на повышенную общественную опасность таких деяний, их высокую латентность.

М. Ю. Дворецкий[16] и В. В. Крылов[17] считают, что существующий подход, согласно которому в уголовном законодательстве следует делать указания на конкретные технические средства, себя уже исчерпал. Понятийно - терминологический аппарат нуждается в реформировании и уточнении, поскольку не отражает существующей действительности. Именно поэтому нецелесообразно

использовать термин «преступления в сфере компьютерной информации» в качестве базового наименования всей совокупности рассматриваемых деяний, так как компьютер при этом является лишь одной из разновидностей информационного оборудования. Проблемами его использования не исчерпывается вся совокупность отношений, связанных с конфиденциальной компьютерной информацией. М. Ю. Дворецкий, используя термин «преступления в сфере информационных ресурсов», а В. В. Крылов, используя термин «информационные преступления» в качестве базового понятия, полагают, что можно абстрагироваться от конкретных технических средств и учесть специфику данных деяний, отграничивая их от других преступлений.

Взяв за основу мнения М. Ю. Дворецкого и В. В. Крылова, Д. В. Добровольский пришел к выводу об обозначении преступлений в сфере компьютерной информации как «преступлений в сфере информационных технологий», под которыми автор предлагает понимать «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 здоровью, правам и свободам человека и гражданина, национальной безопасности»[18].

Д. В. Добровольский полагает, что термин «преступления в сфере компьютерной информации», учитывая, что «компьютеры используются практически во всех сферах жизнедеятельности общества», «не дает возможности четко определить конкретный вид преступлений, приводит к неоднозначности»[19].

Соглашаясь с целесообразностью введения в уголовное законодательство термина «преступления в сфере информационных технологий», отметим, что в таком случае объектом уголовно - правовой охраны будет выступать безопасность в сфере информационных технологий применительно к правам и интересам личности, общества и государства.

Классификация компьютерных преступлений

Компьютерная информация (в соответствии со ст.2 закона «Об информации, информатизации и защите информации”) - это информация о лицах, предметах,

фактах, событиях, явлениях и процессах автономно от формы их отображения, но согласно освещенным статьям под компьютерной информацией толкуются не сами сведения, а форма их отображения в машиночитаемом виде, т.е. множество символов, находящихся в памяти компьютера, либо на машинном носителе[20]..

Компьютерные преступления можно разделить на две большие группы - преступления, связанные с вмешательством в работу компьютеров, и преступления, использующие компьютеры как необходимые технические средства. Лица, которые совершают преступления в компьютерной сфере:

1. Хакеры

2. Психически больные лица, страдающие компьютерными фобиями

3. Криминальные профессионалы

Перечислю некоторые основные виды преступлений, связанных с вмешательством в работу компьютеров[21].

1) Несанкционированный доступ к информации, хранящейся в компьютере включает следующие виды:

1. «За дураком»: 1) физический вариант – проникновение в помещения, где установлены компьютеры, следом за законным пользователем; 2) электронный вариант – подключение терминала незаконного пользователя к линии связи законного пользователя в начале работы или при прерывании активного режима.

2. «За хвост». Перехват сигнала, обозначающего конец работы законного пользователя с последующим осуществлением доступа к системе.

3. «Абордаж». Хакеры часто проникают в чужие информационные системы, подбирая номера на удачу, угадывая коды и т.п.

4. «Неспешный выбор». Несанкционированный доступ к файлам законного пользователя осуществляется нахождением слабых мест в защите системы. Однажды обнаружив их, нарушитель может не спеша исследовать содержащуюся в системе информацию, копировать ее, возвращаться к ней многократно.

5. «Брешь». В отличие от «неспешного выбора», где ищутся слабые места в защите системы, при данном способе производится поиск брешей, обусловленных ошибками или неудачной логикой построения программы.

6. «Люк». «Люк» – это развитие приема «брешь». В найденной бреши программа «развивается», и туда дополнительно вставляют одну или несколько команд. Люк «открывается» по мере необходимости, а встроенные команды автоматически осуществляют свою задачу.

7. «Системные ротозеи». Расчет на неадекватную проверку полномочий пользователя (имена, коды, шифр-ключи и т. п.). Несанкционированный доступ осуществляется нахождением бреши в программе входа в систему.

8. «Маскарад»: 1) физический вариант – для получения информации злоумышленники выдают себя за других лиц, чаще всего за журналистов; 2) электронный вариант – проникновение в компьютерную систему по кодам и другим идентификационным шифрам законных пользователей.

9. «Мистификация». Иногда случается, как например с ошибочным телефонными звонками, что пользователь удаленного терминала подключается к чьей-то системе, будучи абсолютно уверенным, что 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 получать некоторую информацию, в частности, коды доступа к данным.

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

3) Разработка и распространение компьютерных вирусов.

4) Преступная небрежность в разработке, изготовлении и эксплуатации программно - вычислительных комплексов, приведшая к тяжким последствиям.

5) Подделка компьютерной информации.

6) Хищение компьютерной информации включает следующие виды:

1. Непосредственный перехват. Осуществляется, как правило, либо через телефонный канал системы, либо подключением к линии принтера.

2. Электромагнитный перехват. Не требует непосредственного подключения к системе и производится улавливанием с помощью специальных средств излучения, производимого центральным процессором, дисплеем, телефоном, принтером и др.

3. «Жучок». Установка микрофона в компьютере с целью перехвата разговоров работающего на ЭВМ персонала.

4. Откачивание данных. Сбор информации, требующейся для получения основных материалов. Часто при этом исследуется не само содержание информации, а схемы ее движения.

5. «Уборка мусора» в электронном варианте представляет собой исследование данных, оставленных в памяти ЭВМ.

Таким образом, мы пришли к выводу, что процесс информатизации общества подводит мир к подъему количества компьютерных преступлений, увеличению их обособленного веса по размерам краденых сумм в общей доле физических потерь от обычных видов преступлений.

Убытки отдельной страны за небольшой промежуток времени могут доходить до гигантских размеров.

Таким примером служит — уголовное дело о хищении 125,5 тыс. долл. США и подготовке к хищению еще свыше 500 тыс. долл. во Внешэкономбанке СССР в 1991 г., рассмотренное московским судом. По материалам другого уголовного дела, в сентябре 1993 г. было совершено покушение на хищение денежных средств в особо крупных размерах из Главного расчетно - кассового центра Центрального банка России по г.Москве на сумму 68 млрд. 309 млн.768 тыс. руб.[22].

Противоречивость компьютерных преступлений сводится к тому, что тяжело отыскать иной вид преступления, после совершения которого его потерпевший не слишком заинтересован в поимке преступника, а сам преступник, будучи пойман, всеми правдами и неправдами продвигает свою активность в области компьютерного взлома, лишь в малом количестве утаивая от представителей правоохранительных органов.

За преступления в сфере компьютерной информации предусмотрена уголовная ответственность.

Глава 2. Анализ способов совершения компьютерных преступлений

2.1. Технологии сокрытия личности преступников

Описание способов компьютерных преступлений начнем с действий по сокрытию преступниками своих данных при использовании сети Интернет с целью предотвращения идентификации их личности. Для сокрытия своего адреса преступники используют различные анонимные компьютерные сети и сервисы, специально созданные для этих целей.

Одним из таких способов является использование VPN-сервисов (англ. Virtual Private Network — виртуальная частная сеть)[23]. Технологии VPN обеспечивают шифрование сетевого трафика между компьютером пользователя и VPN-прокси-сервером, который является шлюзом выхода в сеть Интернет и, соответственно, скрывает реальный IP-адрес пользователя. Если требуется высокий уровень конспирации, преступники арендуют у провайдеров хостинговых услуг вычислительные мощности практически в любой точке мира, на которых настраивают собственные VPN-серверы либо виртуальные машины, с которых, используя сторонние VPN- сервисы, выходят в сеть Интернет.

Другой способ, использование которого позволяет скрыть свой IP-адрес, — The Onion Routng, TOR (луковая маршрутизация второго поколения), это технология и программное обеспечение для обмена данными с многослойным шифрованием с помощью системы прокси-серверов, обеспечивающих анонимное сетевое подключение[24].

Троянская программа, обладающая функциональными возможностями VPN-прокси-сервера, также позволяет преступникам создать бот-сеть из компьютеров, зараженных такой программой, и использовать ее для сокрытия своего IP-адреса.

Помимо упомянутых способов анонимизации своих действий в сети Интернет путем построения цепочки прокси-серверов, преступники для этих целей применяют и другие криминальные либо полукриминальные схемы, например через несанкционированное подключение к сторонним беспроводным точкам доступа (Wi-Fi-роутерам) или с помощью беспроводных модемов мобильной связи с сим-картами, оформленными на посторонних лиц.

Выбор безопасных способов оплаты сервисов и вычислительных мощностей для осуществления преступной деятельности также является мерой конспирации преступной деятельности. Для этих целей широко используется так называемая

криптовалюта, например биткоины, правовой режим которой во многих странах мира, в том числе в России, остается неопределенным.

Разработка планов преступной деятельности, координация мероприятий на стадии подготовки к совершению преступления, согласование совместных действий осуществляются соучастниками с применением сетевых протоколов обмена сообщениями, обеспечивающих безопасность передачи данных. Одной из наиболее востребованных реализаций коммуникации в криминальной среде является XMPP-протокол (eXtensible Messaging and Presence Protocol) обмена мгновенными сообщениями, известный еще как Jabber-протокол (буквально — болтовня), который предоставляет возможность настроить свой собственный Jabber-сервер, обеспечивающий шифрование канала[25].

К мерам по сокрытию следов преступления можно отнести также способы, с помощью которых преступники оказывают противодействие осмотру и изъятию компьютерной информации, содержащейся в их компьютерных средствах и системах, имеющей криминалистическое значение. Эти цели достигаются шифрованием компьютерных данных с помощью специализированного программного обеспечения либо возможностью быстрого уничтожения таких данных с использованием специальных программ или устройств.

Для сокрытия следов несанкционированного доступа и вредоносной активности на компьютере пользователя применяются различные меры технического характера, как прошедшие проверку временем технологии шифрования (криптования) и обфускации (obfuscate — делать неочевидным, запутанным), так и новые приемы и методы — «бестелесная» технология, технологии Bootkit, Rootkit и т.п.

В процессе криптования исполняемый код вредоносной программы шифруется, а при обфускации приводится к виду, затрудняющему анализ и понимание алгоритмов его работы. Это осложняет выявление таких программ антивирусным программным обеспечением и их исследование специалистами по информационной безопасности.

Вредоносные программы, функционирующие только в оперативной памяти компьютера и не сохраняющиеся на энергонезависимых запоминающих устройствах, именуют «бестелесными». При отключении питания компьютера, например при его перезагрузке, программа стирается. Такие программы используются преступниками для сокрытия своей активности от антивирусного программного обеспечения[26].

2.2. Технологии несанкционированного доступа в глобальной сети Интернет

Технология Bootkit применяется для сокрытия вредоносного кода от антивирусного программного обеспечения и для получения максимальных привилегий в системе. Для реализации этого способа вредоносной программой модифицируется, например, главная загрузочная запись (англ. master boot record, MBR), которая считывается процессором еще до начала загрузки операционной системы, а вредоносный код в зашифрованном виде записывается в не используемую операционной системой область дискового пространства. При включении компьютера загрузчик еще до старта операционной системы расшифровывает и загружает в оперативную память вредоносный код[27].

Максимальные права пользователя позволяют применить набор программ Rootkit, которые скрывают вредоносную активность в системе: сетевые подключения, процессы, файлы и т.д.

Как видно из перечисленных мер, предпринимаемых преступниками с целью сокрытия следов несанкционированного доступа к компьютерным системам и информации пользователя, весьма значительное количество таких деяний совершается с помощью вредоносного программного обеспечения. Преступники используют вредоносные программы для значительного усиления своих возможностей, то есть в криминалистическом плане вредоносная программа является орудием совершения преступления[28].

Заметим, что в качестве орудия совершения преступления может быть использована и легальная программа, функциональность которой предоставляет преступникам возможность достижения своих целей. Большинство легальных программ, используемых преступниками в противоправной деятельности, предназначены для удаленного несанкционированного доступа к компьютеру, управления системой и ее администрирования, например: RMS, Ammyy Admin, TeamViewer и LiteManager. Эти программы обладают функциональными возможностями, достаточными для достижения преступных целей, и определяются антивирусным программным обеспечением с менее критичным именем как условно опасные, в связи с чем пользователи не видят в них особой угрозы. Кроме того, многие из этих программ являются доверенными программами пользователя, установлены с его ведома и не вызывают у него подозрений.

В определенных случаях, например, когда необходимо отключить оповещение пользователя о работе программы либо ее модулей, такие программы подвергаются незначительной модификации, которая может привести к изменению их поведения (набора действий) в системе, которое будет соответствовать другому классу определяемых антивирусным программным обеспечением объектов — Malware (категории вредоносных программ).

Один из таких способов реализуется с помощью технологии DLL Hijacking[29], эксплуатирующей особенности функционирования операционной системы (ОС) Windows. Способ заключается в помещении в одну папку с файлом программы удаленного управления вредоносного библиотечного файла (dll-библиотеки), причем с таким же именем, что и расположенная в другой директории легальная библиотека. При запуске программа вместо легальной библиотеки загружает вредоносную, которая размещена «ближе». Например, для сокрытия от пользователя отображаемых на экране графических признаков работы программы Team Viewer (значка, окна сообщений) преступники осуществляют подмену библиотеки msvfw32.dll.

Самая общая классификация, широко применяемая в настоящее время для систематизации видов вредоносных программ, выделяет из класса вредоносных программ (Malware) следующие подклассы: программы-вирусы (Virus), программы-черви (Worm) и троянские программы (Trojan)[30].

К вирусам относятся программы, которые обладают способностью к саморазмножению и распространению по локальным ресурсам компьютера. Программы-черви способны к саморазмножению и распространению по компьютерным сетям. Таким образом, два подкласса вредоносных программ — вирусы и черви — без ведома пользователя саморазмножаются на компьютерах и в компьютерных сетях, при этом каждая последующая копия также обладает способностью к саморазмножению.

Проиллюстрируем это на примере. В мае 2017 г. была осуществлена одна из наиболее масштабных за обозримое время атака с применением программы-шифровальщика WannaCry. Только за один день эта вредоносная программа атаковала компьютеры пользователей более чем в 74 странах. По своему основному предназначению WannaCry имеет те же функциональные возможности, что и другие шифровальщики: модификация пользовательских данных на компьютере и последующее требование выкупа за их восстановление, но столь массовые случаи заражения были связаны со способом распространения.

Первичное заражение осуществлялось посредством эксплуатации уязвимости ОС Windows. После успешного проникновения хотя бы на один компьютер, подключенный к локальной сети, шифровальщик WannaCry распространялся по сети на другие устройства как червь (Worm). По этой причине наибольший ущерб от шифровальщика WannaCry был причинен организациям, имеющим крупные корпоративные компьютерные сети[31].

Программы, относящиеся к третьему подклассу, — троянские программы — не умеют создавать свои копии и неспособны к самовоспроизведению. В этом случае распространение копий по сети и заражение удаленных компьютеров происходит по команде с сервера управления.

Основным признаком, который служит для дифференцирования троянских программ, является вид действия (поведение), которое они выполняют на компьютере, например:

- программы-шпионы (Trojan-Spy) предназначаются для ведения электронного шпионажа за пользователем, в том числе для перехвата вводимых с клавиатуры данных, изображений экрана, списка активных приложений;
- программы-банкеры (Trojan-Banker) создаются с целью поиска и копирования пользовательской информации, относящейся к банковским счетам, системам электронных денег и пластиковым картам;
- программы-шифровальщики (Trojan-Ransom) модифицируют пользовательские данные на компьютере либо блокируют работу компьютера с целью получения выкупа за восстановление доступа к информации;
- программы для удаленного управления (Trojan-Backdoor) обеспечивают скрытое удаленное управление компьютером и полный доступ к пользовательской информации;
- программы-загрузчики (Trojan-Downloader, Trojan-Dropper) осуществляют загрузку и установку на компьютер вредоносных программ и их новых версий;
- программы для эксплуатации программных уязвимостей (Exploit) эксплуатируют уязвимости программного обеспечения пользователя.

Большинство современных троянских программ сочетают в себе не одно поведение, а целый набор видов деятельности, предоставляющий преступникам самые широкие возможности для манипулирования пользовательской информацией. Например, программа-банкер, определяемая антивирусным программным обеспечением Лаборатории Касперского с именем Trojan-Banker.Win32.RTM, помимо присущей только этому виду троянских программ

функциональности поиска и копирования пользовательской информации, относящейся к банковским счетам, системам электронных денег и пластиковым картам, обладает и многими другими возможностями: поиск файлов по именам, запись истории нажатий клавиш клавиатуры, запись видео и создание снимков экрана, копирование буфера обмена, блокирование и нарушение работы операционной системы, получение от сервера управления команд на запуск дополнительных программных модулей, отправка собранной информации на сервер управления и т.п.

Для загрузки троянских программ в компьютерную систему без ведома пользователя применяют различные способы:

- рассылка электронных писем, содержащих вредоносное вложение;
- применение связок эксплойтов при веб-сер- финге пользователей в сети Интернет;
- внедрение вредоносного кода в распространяемое легальное программное обеспечение;
- распространение в локальной сети посредством применения штатных программных средств;
- физический доступ к целевой системе.

Для проникновения в систему с помощью сообщений электронной почты преступники осуществляют целевую либо массированную рассылку писем, содержащих в качестве вложения специальным образом сформированный документ. Открытие пользователем данного документа приводит к скрытой загрузке вредоносной программы и установке ее в систему. В другом варианте вредоносное письмо содержит не вложение, а ссылку на внешний интернет-ресурс, при переходе по которой компьютер пользователя подвергается атаке набором эксплойтов. При успешном срабатывании одного из эксплойтов на компьютер пользователя загружается вредоносное программное обеспечение. При необходимости, когда возможности совершения несанкционированных действий

на компьютере пользователя ограничены правами его учетной записи, преступниками может быть применен локальный эксплойт для повышения привилегий.

Для заражения компьютеров может быть использован так называемый метод drive-by-загрузки, когда в процессе перемещения пользователя по сайтам в сети Интернет его компьютер скрыто перенаправляется с легитимной, но

скомпрометированной страницы на криминальный ресурс, где подвергается атаке набором эксплойтов.

Описанные способы наиболее распространены и хорошо известны. В более редких случаях преступники предварительно получают несанкционированный доступ к сетевым ресурсам разработчика легальных программ, после чего внедряют в распространяемое им программное обеспечение свой вредоносный код.

При наличии у преступников доступа хотя бы к одному компьютерному устройству локальной сети организации дальнейшее распространение вредоносных программ на другие компьютеры и серверы может осуществляться с помощью штатных программных средств и протоколов. Например, неоднократно фиксировалось использование программы PsExec от корпорации Microsof для автоматизированного развертывания вредоносного программного обеспечения на всех компьютерах, входящих в корпоративную сеть.

Физический доступ к компьютерной системе может быть обеспечен вовлечением в преступление работника потерпевшей организации либо проникновением преступников за охраняемый периметр. В этом случае загрузка вредоносной программы в систему осуществляется посредством подключения к ней внешнего электронного носителя информации.

Помимо программных средств, в более редких случаях способами компьютерных преступлений служат специально созданные в преступных целях электронно-вычислительные устройства и программы к ним. Подобные комплексы могут быть как достаточно простыми (например, устройство, скрыто устанавливающееся в разрыв интерфейса клавиатуры для перехвата нажатия клавиш), так и более сложными (например, компьютерное устройство размером с USB-флеш-накопитель с собственным сетевым адаптером и установленной специальной программой удаленного управления предоставляет преступнику возможность получить несанкционированный доступ к удаленной компьютерной системе; для этого устройство скрыто подключается к целевой системе, например корпоративной компьютерной сети, в месте, исключающем его визуальное обнаружение, для чего нередко в преступление вовлекают работника пострадавшей организации).

К более сложным техническим решениям, создаваемым для совершения преступлений, применимо иное название — аппаратно-программные комплексы. К ним относятся так называемые бот-фермы, то есть компьютерные системы, эмулирующие работу большого количества устройств с отдельными каналами

подключения к сети Интернет. Такие системы используются для массовых кампаний распространения вредоносного программного обеспечения на мобильные устройства под управлением ОС Android посредством СМС-рассылки либо для DDoS-атак.

Весьма существенную угрозу для банковской сферы представляют аппаратно-программные комплексы, разработанные для хищения денежных средств из банкоматов, — так называемые Black Box. Такой комплекс является, по сути, мини-компьютером со специальным программным обеспечением, который подключают к диспенсеру (механизму выдачи денег) вместо штатного компьютера, расположенного в сервисной зоне банкомата. После этого управление банкоматом может осуществляться с помощью технологий беспроводной передачи данных, например со смартфона.

2.3. Технологии несанкционированного доступа в локальных сетях

Глобальная сеть Интернет является всемирной системой объединенных компьютерных сетей, поэтому представляется необходимым уделить внимание таким способам осуществления несанкционированного доступа, как компьютерные атаки на локальные сети.

Согласно Национальному стандарту ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения»[32] «под компьютерной атакой понимается целенаправленное несанкционированное воздействие на информацию, на ресурс автоматизированной информационной системы или получение несанкционированного доступа к ним с применением программных или программно-аппаратных средств» (п. 3.11). Фактически под признаки компьютерной атаки подпадают все способы осуществления несанкционированного доступа к компьютерным системам, упомянутые в настоящей статье. Однако именно атаки на локальные сети позволяют наиболее полно рассмотреть приемы и методы, используемые преступниками с этой целью.

Виды компьютерных атак на локальные корпоративные сети могут быть разными:

- внешняя атака на сетевую инфраструктуру организации либо на компьютерные системы, которым разрешено удаленное подключение к

локальной сети;
- атака изнутри пострадавшей организации с участием ее работников;
- комбинированная атака, сочетающая в себе элементы обоих указанных выше способов совершения преступления.

Необходимо учитывать, что преступник, действующий внутри организации, может также использовать вредоносные программы, как и преступник внешний. С одной стороны, это усиливает его возможности, с другой — может ввести в заблуждение следствие относительно участия в преступлении инсайдера, если такие программы будут обнаружены в ходе осмотра места происшествия и при проведении судебной экспертизы. Участие инсайдера в преступлении не обязательно должно быть непосредственным. Работник организации может предоставить соучастникам необходимые сведения для осуществления несанкционированного доступа внутрь корпоративной компьютерной сети или сообщить об уязвимостях программного обеспечения, установленного на компьютерах организации, либо ошибках в настройках сетевого оборудования.

Функциональные возможности вредоносных программ и легальных условно опасных программ, предоставляющих удаленный доступ к системе, позволяют проводить атаки на компьютерные системы без какого-либо вовлечения в этот процесс потерпевших. В этом случае реализация преступного умысла осуществляется втайне от них, а зачастую скрыта и от третьих лиц, так как происходит только на уровне машинной обработки и передачи компьютерной информации.

На этой основе способы компьютерных преступлений в зависимости от доступа к компьютерным средствам и системам можно подразделить:

- на способы, связанные с удаленным доступом к компьютерным средствам и системам посредством использования компьютерной коммуникационной сети (локальной или глобальной — Интернет);
- способы, связанные с непосредственным доступом к компьютерным средствам и системам.

В других случаях вовлечение потерпевшего, в той или иной степени, является необходимым условием доведения преступных намерений до конца. Непосредственная эксплуатация уязвимостей человеческого фактора предусматривает прямое общение с потерпевшим с применением навыков социальной инженерии, то есть системы психологических приемов и методов,

склоняющих потерпевших к совершению определенных действий в интересах преступников, например к разглашению уникального кода, присланного в СМС-сообщении для авторизации на сетевом ресурсе, либо к самостоятельной загрузке программы удаленного администрирования на свой компьютер и предоставлению реквизитов доступа к нему мошеннику.

Однако низкий уровень культуры информационной безопасности позволяет преступникам получать необходимые сведения для проведения атаки и без прямого общения с потерпевшим. Использование ненадежных паролей, заводских настроек и конфигураций программного обеспечения и оборудования предоставляет широкий спектр возможностей для получения несанкционированного доступа к конфиденциальной информации. Так, один из широко известных и применяемых способов получения несанкционированного доступа к компьютерной сети — это проведение атаки с применением различных методов сканирования портов сетевых узлов, то есть виртуальных точек входа-выхода сетевого трафика, обслуживающих определенные локальные сервисы. Обнаружив в результате сканирования открытый порт, который обычно используется одной из распространенных программ удаленного администрирования, преступники могут получить доступ к системе перебором реквизитов доступа (пары логин — пароль).

Для доступа к корпоративным компьютерным системам преступники могут воспользоваться и уязвимостью в организации охранных систем и регламентов предприятия, что может выражаться как в физическом проникновении за охраняемый периметр, так и в удаленном доступе с использованием разрешенных в организации к применению протоколов и программных средств. В связи с этим можно разграничить способы получения несанкционированного доступа к компьютерным системам и сетям по степени вовлеченности протерпевшего в этот процесс:

- эксплуатация уязвимостей аппаратного и программного обеспечения;
- использование недостатков организационного и технического характера корпоративных охранных систем;
- применение методов социальной инженерии.

Заключение

Вследствие продолжающегося бурного развития информационно-коммуникационных технологий, в том числе средств криптографии, такая же ди намика присутствует и в освоении преступниками способов компьютерных преступлений, сопряженных с несанкционированным доступом к компьютерным средствам и системам. При этом отходят на второй план и используются только в качестве вспомогательных распространенные еще в недавнем прошлом способы преступлений, такие как, например, перехват сетевого трафика, потерявший свою эффективность с точки зрения преступников в результате массового перехода сетевых сервисов с HTTP- протокола, предусматривающего открытую передачу данных, на протокол HTTPS, обеспечивающий шифрование сетевого трафика между конечными устройствами.

Статистика компьютерной преступности РФ характеризуется следующим образом:

- экономические преступления – 67%;
- политические преступления – 17%;
- исследовательский интерес – 6%;
- месть – 5%;
- хулиганство – 5%.

Наиболее широко распространенные экономические преступления в основном с вязаны с теми или иными способами хищения денежных средств. Больше трех лет назад появился известный вирус «AndroidOsSelektor», который блокировал возможность чтения пользователем мобильного банка сообщений о снятии денег с его счета или переводов с его карты на другие платежные карты или счета, а также эмулировал (без ведома пользователя) отправление SMS-сообщений с необходимым для этих операций паролем. Этот первый вирус в РФ «снял» более 70000 руб. у четырех первых «счастливчиков», у которых смартфон с Андроидом заразился этим вирусом. Участились случаи заражения аналогами данного вируса особенно в последнее время.

Действенным средством против таких вирусов является «привязка» мобильного банка к таким телефонам, на которых нет Андроида, Windows SE и т.п. развитых операционных систем, в которых вирус способен существовать и действовать. Данные вирусы не способны к существованию в среде тривиальных, простейших операционных систем, таких как, например, DOS. Следовательно, для «привязки» мобильного банка необходим простейший «кнопочный» сотовый телефон, в котором нет указанных выше операционных систем, и в котором вирус не может существовать.

Список использованных источников

1. Уголовный кодекс РФ
2. Федеральный закон «Об информации, информатизации и защите информации» от 27.07.2006 № 149 - ФЗ, ст.2
3. ГОСТ Р 51275-2006. Национальный стандарт Российской Федерации. «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» (утв. и введен в действие приказом Ростехрегулирования от 27.12.2006 № 374 ст).
4. Батурин, Ю. М. Компьютерная преступность и компьютерная безопасность / Ю. М. Батурин, А. М. Жодзишский. - М.: Инфра-М, 2016. – 421 с.
5. Богданова Н. К вопросу об определении понятия «Преступления в сфере компьютерной информации» // Вестник Челябинского государственного университета. 2017. № 37 (291)
6. Вехов, В. Б. Компьютерные преступления: Способы совершения. Методики расследования. - М.: Инфра-М, 2016. – 245 с.
7. Вехов, В.Б. Особенности расследования преступлений, совершаемых с использованием средств электронно-вычислительной техники.- М.: Кнорус , 2016. - С. 6
8. Дворецкий, М. Ю. Преступления в сфере компьютерной информации: понятие, система, проблемы квалификации и наказания.- Тамбов, 2015. С. 13
9. Комиссаров, В. С. Преступления в сфере компьютерной безопасности; понятие и ответственность // Юрид. мир. 2018. № 2. - С. 22
10. Копылов, В. А. Информационное право: вопросы теории и практики. - М.: Кнорус, 2015. - 614 с.
11. Крылов, В. В. Информационные преступления — новый криминалистический объект // Рос.юстиция. 2017. № 4. - С. 22–23
12. Крылов, В. В. Расследование преступлений в сфере информации. - М.: Кнорус, 2018. - С. 162
13. Куроуз Д., Росс К. Компьютерные сети: нисходящий подход. 6-е изд. М., 2016. С. 794—795.
14. Курушин, В. Д. Компьютерные преступления и информационная безопасность / В. Д. Курушин, В. А. Минаев. - М.: Кнорус, 2018. - С. 48.
15. Ляпунов, Ю. Ответственность за компьютерные преступления / Ю. Ляпунов, В. Максимов //Законность. 2017. № 1. - С. 9

16. Мнацаканян А. В. – Преступения в сфере безопасности компьютерной информации как элемент системы Особенной части Уголовного Кодекса Российской Федерации // Пробелы в российском законодательстве, 2017.
17. Пархомов, В. А. К определению понятия «информационное преступление» / // Вестн. Иркутск.гос. экон. акад. 2017. № 1. - С. 92–96
18. Расследование преступлений повышенной общественной опасности : пособие для следователя / под ред. Н. А. Селиванова, А. И. Дворкина.- М.: Инфра-М, 2018. - 334 с.
19. Селиванов, Н. Проблемы борьбы с компьютерной преступностью // Законность. 2015. № 8. - С. 37
20. Талимончик В.П. Компьютерные преступления и новые проблемы сотрудничества государств//Законодательство и экономика, 2015, №5
21. Торичко Р. С., Клишина Н. Е. Некоторые вопросы совершенствования действующего законодательства, регламентирующего расследование киберпреступлений // Вестник экономической безопасности. 2018. № 3. С. 181
22. Чекунов И. Г. Современные киберугрозы. Уголовно-правовая и криминологическая классификация и квалификация киберпреступлений // Право и кибербезопасность. 2012. № 1. С. 9—22.
23. Чекунов И. Г., Рядовский И. А., Иванов М. А. [и др.] Методические рекомендации по расследованию преступлений в сфере компьютерной информации : учеб. пособие / под ред. И. Г. Чекунова. М. : Московский университет МВД России имени В. Я. Кикотя, 2018. С. 28—29
24. Энциклопедия Лаборатории Касперского. Классификация детектируемых объектов. Вредоносные программы // URL: https://encyclopedia.kaspersky.ru/knowledge/malicious-programs
25. Ligh M., Ad air S., Hartstein B., Richard M. Malware Analyst’s Cookbook and DVD: Tools and Techniques for Fighting Malicious Code. Indianapolis, 2010. Pp. 2—5.
26. Matrosov A., Rodionov E., Bratus S. Rootkits and Bootkits: Reversing Modern Malware and Next Generation Threats. No Starch Press, 2015. P. 304
27. The MITRE Corporation. CWE-427: Uncontrolled Search Path Element // URL: https://cwe.mitre.org/data/ definitions/427.html
28. Zeltser L. The History of Fileless Malware — Looking Beyond the Buzzword // URL: https://zeltser.com/fileless- malware-beyond-buzzword
29. Компьютерные преступления. URL: http: // www.grandars.ru
30. Компьютерные преступления. URL: https: // www.zonazakona.ru

1. Мнацаканян А. В. – Преступения в сфере безопасности компьютерной информации как элемент системы Особенной части Уголовного Кодекса Российской Федерации // Пробелы в российском законодательстве, 2017. ↑

2. Курушин, В. Д. Компьютерные преступления и информационная безопасность / В. Д. Курушин, В. А. Минаев. - М.: Кнорус, 2018. - С. 48. ↑

3. . Богданова Н. К вопросу об определении понятия «Преступления в сфере компьютерной информации» // Вестник Челябинского государственного университета. 2017. № 37 (291) ↑

4. Талимончик В.П. Компьютерные преступления и новые проблемы сотрудничества государств//Законодательство и экономика, 2015, №5 ↑

5. Батурин, Ю. М. Компьютерная преступность и компьютерная безопасность / Ю. М. Батурин, А. М. Жодзишский. - М.: Инфра-М, 2016. – 421 с. ↑

6. Уголовный кодекс РФ ↑

7. Вехов, В.Б. Особенности расследования преступлений, совершаемых с использованием средств электронно-вычислительной техники.- М.: Кнорус , 2016. - С. 6 ↑

8. Ляпунов, Ю. Ответственность за компьютерные преступления / Ю. Ляпунов, В. Максимов //Законность. 2017. № 1. - С. 9 ↑

9. Селиванов, Н. Проблемы борьбы с компьютерной преступностью // Законность. 2015. № 8. - С. 37 ↑

10. Вехов, В. Б. Компьютерные преступления: Способы совершения. Методики расследования. - М.: Инфра-М, 2016. – 245 с. ↑

11. Копылов, В. А. Информационное право: вопросы теории и практики. - М.: Кнорус, 2015. - 614 с. ↑

12. Крылов, В. В. Информационные преступления — новый криминалистический объект // Рос.юстиция. 2017. № 4. - С. 22–23 ↑

13. Пархомов, В. А. К определению понятия «информационное преступление» / // Вестн. Иркутск.гос. экон. акад. 2017. № 1. - С. 92–96 ↑

14. Расследование преступлений повышенной общественной опасности : пособие для следователя / под ред. Н. А. Селиванова, А. И. Дворкина.- М.: Инфра-М, 2018. - 334 с. ↑

15. Комиссаров, В. С. Преступления в сфере компьютерной безопасности; понятие и ответственность // Юрид. мир. 2018. № 2. - С. 22 ↑

16. Дворецкий, М. Ю. Преступления в сфере компьютерной информации: понятие, система, проблемы квалификации и наказания.- Тамбов, 2015. С. 13 ↑

17. Крылов, В. В. Расследование преступлений в сфере информации. - М.: Кнорус, 2018. - С. 162 ↑

18. Крылов, В. В. Расследование преступлений в сфере информации. - М.: Кнорус, 2018. - С. 162 ↑

19. Дворецкий, М. Ю. Преступления в сфере компьютерной информации: понятие, система, проблемы квалификации и наказания.- Тамбов, 2015. С. 13 ↑

20. Федеральный закон «Об информации, информатизации и защите информации» от 27.07.2006 № 149 - ФЗ, ст.2 ↑

21. Компьютерные преступления. URL: http: // www.grandars.ru ↑

22. Компьютерные преступления. URL: https: // www.zonazakona.ru ↑

23. *Куроуз Д., Росс К.* Компьютерные сети: нисходящий подход. 6-е изд. М., 2016. С. 794—795. ↑

24. *Ligh M., Ad air S.*, *Hartstein B.*, *Richard M.* Malware Analyst’s Cookbook and DVD: Tools and Techniques for Fighting Malicious Code. Indianapolis, 2010. Pp. 2—5. ↑

25. *Торичко Р. С., Клишина Н. Е.* Некоторые вопросы совершенствования действующего законодательства, регламентирующего расследование киберпреступлений // Вестник экономической безопасности. 2018. № 3. С. 181 ↑

26. *Zeltser L.* The History of Fileless Malware — Looking Beyond the Buzzword // URL: https://zeltser.com/fileless- malware-beyond-buzzword ↑

27. *Matrosov A., Rodionov E.*, *Bratus S.* Rootkits and Bootkits: Reversing Modern Malware and Next Generation Threats. No Starch Press, 2015. P. 304 ↑

28. *Чекунов И. Г.* Современные киберугрозы. Уголовно-правовая и криминологическая классификация и квалификация киберпреступлений // Право и кибербезопасность. 2012. № 1. С. 9—22. ↑

29. The MITRE Corporation. CWE-427: Uncontrolled Search Path Element // URL: https://cwe.mitre.org/data/ definitions/427.html ↑

30. Энциклопедия Лаборатории Касперского. Классификация детектируемых объектов. Вредоносные программы // URL: https://encyclopedia.kaspersky.ru/knowledge/malicious-programs ↑

31. *Чекунов И. Г., Рядовский И. А.*, *Иванов М. А.* [и др.] Методические рекомендации по расследованию преступлений в сфере компьютерной информации : учеб. пособие / под ред. И. Г. Чекунова. М. : Московский университет МВД России имени В. Я. Кикотя, 2018. С. 28—29 ↑

32. ГОСТ Р 51275-2006. Национальный стандарт Российской Федерации. «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» (утв. и введен в действие приказом Ростехрегулирования от 27.12.2006 № 374 ст). ↑