УДК 34

ПЕРСПЕКТИВЫ РАЗВИТИЯ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕЛЕГАЛЬНОГО КОПИРОВАНИЯ. ТЕОРЕТИЧЕСКИЙ АСПЕКТ ПРОБЛЕМЫ

Самогин А.С.

методист кафедры КБ-13, студент

ФГБОУ ВО "Московский технологический университет"

г. Москва, Россия

Аннотация

В настоящей работе рассмотрен вопрос технического регулирования утечки информации, классификации угроз, в контексте защиты информации от несанкционированного доступа через сети интернет. Также автор акцентирует внимание на правах и обязанностях участников интернет-сообщества по защите компьютеров от несанкционированного доступа, методах и способах защиты информации от несанкционированного доступа. Проблемы утечки информации могут разделяться на технические и гуманитарные. Теория перехвата данных появилась задолго до начала компьютерной эры. В статье анализируется теоретический опыт перехвата информации в связи с деятельностью в современной сети Интернет.

Ключевые слова: юридическое лицо, физическое лицо, интернет, хакеры, защита информации, гражданское право.

PROSPECTS FOR THE DEVELOPMENT OF INFORMATION PROTECTION FROM ILLEGAL COPYING. THEORETICAL ASPECT OF THE PROBLEM

Samogin A.S.
methodist, student
Moscow Technological University (MIREA)
Moscow, Russia

Abstract
In this paper we consider the issue of technical regulation of information leakage, classification of threats in the context of information protection from unauthorized access via the Internet. The author also focuses on the rights and obligations of members of the Internet community to protect computers from unauthorized access, methods and methods of protecting information from unauthorized access. Problems of information leakage can be divided into technical and humanitarian. The theory of data interception appeared long before the beginning of the computer era. The article analyzes the theoretical experience of interception of information in connection with the activities in the modern Internet.

Keywords: legal entity, individual, Internet, hackers, information protection, civil law.

В современном мире вопросы защиты информации играют чрезвычайно важную роль. Этим определяется актуальность темы работы, которая носит название «Перспективы развития защиты информации от нелегального копирования. Теоретический аспект проблемы». Актуален данный порос как для частных лиц, так и для крупных компаний и даже на уровне государства в настоящее время организовываются специальные отделы, которым поручено заниматься вопросами защиты информации.

В рамках данной работы мы разберем возможности защиты информации от несанкционированного доступа с целью определения

особенностей данного вопроса и сформируем соответствующие выводы по рассматриваемой теме.

В качестве материалов для работы будут использованы информационные источники на основе работ специалистов в области информационной безопасности.

Классификация и структура технических каналов утечки информации. Канал утечки информации представляет собой путь от источника информации до получателя информации несанкционированным способом. Обобщенная типовая структура канала передачи информации приведена на рис. 1

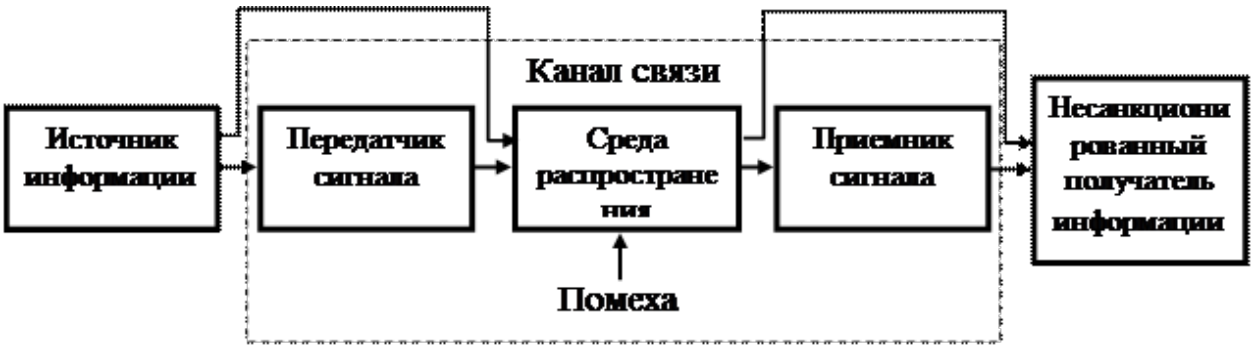

Рис. 1 Структура технического канала утечки информации [2]

Как мы видим, на вход канала поступает информация в виде первичного сигнала. Первичный сигнал представляет собой носитель с информацией от ее источника или с выхода предыдущего канала утечки. Данный источник информации может быть абсолютно любым. Это цель атакующего для получения защищаемой информации. Непосредственно, самих каналов утечки информации может быть несколько, и они могут представлять собой взаимосвязанную цепочку, составляющую целую систему.

Поскольку информация от источника приходит на вход канала на языке источника (в виде буквенно-цифрового текста, символов, знаков, звуков или сигналов), то передатчик производит преобразование этой формы

представления информации в форму, которая обеспечивает запись ее на какой-либо носитель информации, соответствующий среде распространения.

Среда распространения носителя представляет собой такую часть пространства, в которой перемещается носитель. Среда распространения информационного сигнала также может быть различной [3, с. 254].

Главной ролью приемника являются функции, которые противоположны функции передатчика. Он осуществляет выбор необходимого носителя, съем информации с носителя (демодуляцию, декодирование), преобразование информации в форму сигнала, доступную получателю (человеку, техническому устройству), и усиление сигналов до значений, необходимых для безошибочного восприятия ими.

Канал утечки информации имеет некоторые отличия от функционального канала передачи получателем информации. В случае, когда получатель санкционированный, то канал функциональный, иначе он представляет собой канал утечки информации. Классификация каналов утечки информации продемонстрирована на рис. 2.

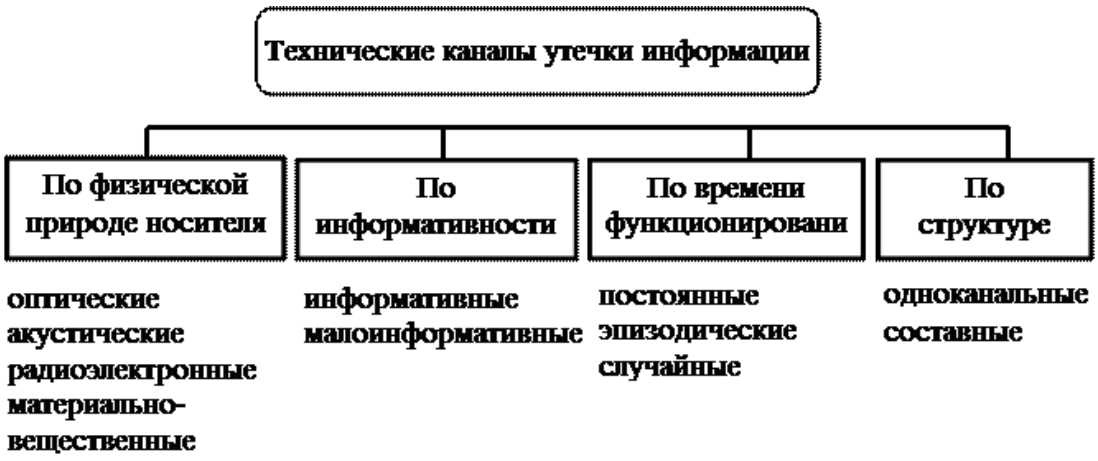

Рис. 2 Классификация технических каналов утечки информации [2]

Основным классификационным признаком технических каналов утечки информации является физическая природа носителя. По данному

признаку они подразделяются на: оптические, радиоэлектронные, акустические, материально-вещественные.

Носителем информации в оптическом канале является электромагнитное поле в диапазоне 0.46-0.76 мкм (видимый свет) и 0.76-13 мкм (инфракрасные излучения) [3, с. 362].

В радиоэлектронном канале утечки информации в качестве носителей используются электрические, магнитные и электромагнитные поля в радиодиапазоне, а также электрический ток, распространяющийся по проводникам.

Носителями информации в акустическом канале являются механические акустические волны в инфразвуковом (менее 16 Гц), звуковом (16 Гц – 20 кГц) и ультразвуковом (свыше 20 кГц) диапазонах частот, способные распространяться в газообразной, жидкой, либо твердой среде [2, с. 121].

В материально-вещественном канале утечка информации происходит за счет несанкционированного распространения за пределы контролируемой зоны носителей с информацией в виде материальных тел (макрочастиц).

По такому параметру как информативность каналы утечки информации подразделяются на информативные, малоинформативные и неинформативные. При этом, информативность канала следует оценивать ценностью информации, передаваемой по каналу связи.

Канал утечки информации, состоящий из передатчика, среды распространения и приемника, является одноканальным. Однако возможны варианты, когда утечка информации происходит более сложным путем - по нескольким последовательным или параллельным каналам. Такие каналы утечки будут называться составными

Таким образом, следует сделать вывод, что канал утечки информации представляет собой некую систему, состоящую из определенных

взаимосвязанных звеньев. В процессе утечки информация постепенно переходит от одного элемента данной системы к другому. В случае, когда на одном из этапов несанкционированного доступа утечка встречает препятствия, то процесс утечки информации нарушается.

Классификация угроз и объектов защиты. Угроза информационной безопасности представляет собой определенный комплекс условий и факторов, которые способны создать потенциальную или реально существующую опасность для защищенности информации от несанкционированного доступа. При этом, источником угрозы информационной безопасности является субъект, способный реализовать негативное воздействие и являющийся причиной угрозы безопасности информации. Источники угроз информационной безопасности чрезвычайно многочисленны и все их перечислить достаточно сложно. Однако они могут быть классифицированы по определенным категориям. Поскольку в данной работе речь идет о защите информации от несанкционированного доступа, то большая часть носителей угроз относится к субъективным. Но несанкционированный доступ к конфиденциальной информации может быть получен и случайным образом какими-либо лицами вследствие объективных причин. Так происходило, например, когда пользователи поисковой системы Google стали обнаруживать в результатах поиска файлы, которые хранят пользователи на облачном хранилище Google и доступ к которым не был защищен. Компания, разумеется, исправила данную ситуацию, однако значительное количество информации оказалось доступным другим лицам. Аналогичные ситуации происходили и с другими поисковыми системами [4, с. 265].

Среди источников угроз информационной безопасности выделяются преднамеренные нарушители конфиденциальности, ошибки проектирования информационных систем, ошибки эксплуатации информационных систем и

т.д. Как правило, наиболее опасными являются преднамеренные нарушители конфиденциальности. Представители данной категории сознательно пытаются получить доступ к защищаемой информации. При этом они используются самые различные способы атак, начиная с социальной инженерии и заканчивая сложными комплексными техническими решениями, которые разрабатываются командами опытных программистов. Источники угроз информационной безопасности должны быть хорошо классифицированы, поскольку это позволяет вырабатывать политику защиты информации и разрабатывать определенные регламенты действий, которые необходимо будет произвести в случае если данные угрозу будут реализованы в действительности.

Угрозы информационной безопасности могут быть классифицированы по различным критериям.

По природе возникновения угрозы могут быть естественными и искусственными.

По степени мотивации - преднамеренными и непреднамеренными.

По положению относительно защищаемой зоны - внутренние и внешние. Так, внешние угрозы могут проявляться через сеть интернет, а источниками внутренних могут стать сотрудники компании.

Отсюда можно сделать вывод, что угрозы информационной безопасности от несанкционированного доступа являются чрезвычайно многочисленными. Для того, чтобы их категоризировать используются соответствующие классификации, которые помогают определять возможные источники угроз и нивелировать вероятность их воздействия на информационные системы.

Методы и способы защиты информации от несанкционированного доступа. Процесс обеспечения защиты информации от несанкционированного доступа является противоположностью методам

взлома информационных систем с целью доступа к информации. И соответственно, существует определенное противостояние специалистов, которые занимаются защитой информации и злоумышленников, пытающихся эту информацию похитить.

Вполне очевидно, что совершенствуются не только методы защиты. Также, становятся все более изощренными техники несанкционированного доступа к информации. И поэтому необходимо чтобы методы защиты постоянно совершенствовались. Для этих целей постоянно ведется работа по поиску уязвимостей в информационных системах компаниями, которые работают в данной сфере.

Прежде всего, следует отметить то, что система защиты информации от несанкционированного доступа должна осуществляться комплексно, поскольку при системе защиты, которая покрывает не весь спектр потенциальных угроз, риски проникновения в систему все равно остаются.

На практике используют различные группы методов защиты. Их можно классифицировать следующим образом.

Каждый из методов защиты информации реализуется при помощи различных категорий средств. Основные средства – организационные и технические. И тем и другим средствам требуется уделять равное количество внимания, поскольку только комплексная система защиты информации способна обеспечить требуемое качество и надежность защиты

Разработкой системы организационных методов защиты информации от несанкционированного входит обычно в компетенцию службы безопасности организации. При этом специалисты по безопасности выполняют следующие функции:

- осуществляют разработку внутренней документации, которая устанавливает регламенты взаимодействия сотрудников с компьютерной техникой и конфиденциальной информацией;

- осуществляют проведение инструктажа и периодических проверок персонала; проводят разработку и подписание дополнительных соглашений к трудовым договорам, в которых определяется ответственность за разглашение или неправомерное использование сведений, которые принадлежат компании и составляют коммерческую тайну;
- производят разграничение зоны ответственности отдельных категорий персонала, чтобы исключить ситуации, когда наиболее важная информация находятся в распоряжении только одного из сотрудников персонала; занимаются организацией работы в общих программах документооборота и проводят мониторинг, чтобы наиболее значимая информация располагалась на необходимых носителях;
- занимаются внедрением программных продуктов, предотвращающих копирование или уничтожения информации любым пользователем, в том числе топ-менеджментом организации;
- занимаются составлением регламентов восстановления систем на случай выхода из строя по каким-либо причинам [2, с. 36].

Категория технических инструментов защиты информации от несанкционированного доступа совмещает аппаратные и программные средства. Основными среди них следует назвать:

- резервное копирование и удаленное хранение наиболее важных массивов данных в компьютерной системе применяется на случай повреждения какой-либо значимой информации. Резервное копирование, вообще, является чрезвычайно важным аспектом функционирования современных информационных систем и ему необходимо уделять предельное количество внимания;
- дублирование и резервирование всех подсистем сетей, которые имеют значение для сохранности данных. Данный момент предполагает наличие каких-либо резервных каналов в сети и резервного оборудования;

- создание возможности перераспределять ресурсы сети в случаях нарушения работоспособности отдельных элементов;
- установка защитного программного обеспечения, которое обеспечивает защиту программного обеспечения операционной системы, баз данных и другой информации от несанкционированного доступа. Следует использовать наиболее продуманные решения в данном вопросе, поскольку большинство подобного программного обеспечения известно злоумышленникам, и они постоянно ищут способы для обхода защитного программного обеспечения, ищут в нем уязвимости [5, с. 62].

В комплекс технических мер входят и меры по обеспечению физической недоступности объектов компьютерных сетей, например, такие практические способы, как оборудование помещения камерами и сигнализацией. Сюда же относится и установка системы управления доступом в помещения, где располагается оборудование, отвечающее за сохранность информации. При этом, необходимо, чтобы присутствовало разграничение возможностей доступа для отдельных категорий сотрудников организации.

Аутентификация и идентификация. Данные способы применяют, чтобы исключить неправомерный доступ к информации открытым способом. Идентификация представляет собой механизм присвоения собственного уникального имени или образа пользователю, который взаимодействует с информацией. Аутентификация – это система способов проверки совпадения пользователя с тем образом, которому разрешен допуск.

Данные средства направлены на то, чтобы предоставить или, наоборот, запретить допуск к данным. Подлинность, как правила, определяется тремя способами: программой, аппаратом, человеком. При этом объектом аутентификации может быть не только человек, но и техническое средство (компьютер, монитор, носители) или данные. Простейший способ защиты –

пароль. Здесь следует отметить то, что вопросу создания паролей следует уделять достаточно пристальное внимание, поскольку ненадежные пароли легко поддаются атакам по методу «грубой силы», которые представляют собой атаки перебора комбинаций паролей по словарям. Разумеется, что не всегда надежный пароль является хорошей защитой, поскольку он все равно может быть украден с помощью троянской программы, либо кейлоггера, поэтому наиболее подверженные атакам объекты защиты необходимо дополнительно защищать, например, методом двойной аутентификации, либо установкой сертификатов безопасности, которые представляют собой криптографические средства защиты [6].

Как отмечают специалисты в области информационной безопасности, наиболее уязвимым звеном любой информационной системы являются люди. Процесс получения несанкционированного доступа к информации без непосредственного использования технических средств и посредством манипуляций с сознательностью сотрудников носит название социальной инженерией. Следует заметить, что социальная инженерия не является какой-либо строгой системой, а методы социальной инженерии ничем не регламентированы. Специалисты по социальной инженерии используют невнимательность сотрудников, халатность, их недостаточную ответственность к выполняемой работе и т.д. Так, известны случаи, когда аудиторы информационной безопасности попросту выносили компьютеры из офиса банка под предлогом необходимости их ремонта, а среди всемирно известных взломов существует немалое количество таких, когда использование специальных программ и применения технических средств вообще не производилось [7].

Для того чтобы препятствовать техникам социальной инженерии требуется строгая регламентация деятельности сотрудников организации, их обучение и контроль за их деятельностью.

В целом же, следует отметить, что способы защиты от возможных атак существуют в очень значительном количестве. Однако они не являются всеобъемлющими и зачастую новые способы защиты от вероятных угроз появляются либо одновременно с выявлением уязвимостей, либо уже после того, как уязвимости были кем-либо использованы. В настоящее время является достаточно распространенной практикой проверка на наличие уязвимостей информационных систем [8]. При этом, профессиональные команды специалистов проводят аудит безопасности определенных систем и предлагают решения для усиления защиты. Также, интересной практикой являются независимые соревнования по поиску уязвимостей крупных ресурсов. Например, такие компании как facebook, Amazon и др предлагают крупные вознаграждения за нахождение уязвимостей в их системах [9].

Угрозы информационной безопасности от несанкционированного доступа являются чрезвычайно многочисленными. Для того, чтобы их категоризировать используются соответствующие классификации, которые помогают определять возможные источники угроз и нивелировать вероятность их воздействия на информационные системы [10].

Способы защиты от возможных атак существуют в очень значительном количестве. Однако они не являются всеобъемлющими и зачастую новые способы защиты от вероятных угроз появляются либо одновременно с выявлением уязвимостей, либо уже после того, как уязвимости были кем-либо использованы. В настоящее время является достаточно распространенной практикой проверка на наличие уязвимостей информационных систем [11]. При этом, профессиональные команды специалистов проводят аудит безопасности определенных систем и предлагают решения для усиления защиты. Также, интересной практикой являются независимые соревнования по поиску уязвимостей крупных

ресурсов. Например, такие компании как facebook, Amazon и др предлагают крупные вознаграждения за нахождение уязвимостей в их системах.

Библиографический список:

1. Мамлюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации: учеб. пособие. - М.: Горячая линия-телеком, 2014 г. - 270 с.
2. Мамаев М. Технологии защиты информации: спец. справочник. - СПб.: ПИТЕР, 2017 г. - 844 с.
3. Мэйволд Э. Безопасность сетей. Шаг за шагом. - М.: СП ЭКОМ, 2015 г. - 547 с.
4. Норткат С. и др. Анализ типовых нарушений безопасности в компьютерных сетях. - М.: Издат. дом «Вильямс», 2017 г. – 470 с.
5. Основы информационной безопасности: [учеб, пособие для вузов] /Е.Б. Белова [и др.]. - М.: Горячая линия - Телеком АРВ, 2006. - 544 с.
6. Петраков Р.В., Лагутина В.С. Защита абонентского телетрафика: учеб. пособие. - М.: Радио и связь, 2014 г. - 479 с.
7. Бабенко М.И. Хакер. Взлом и защита. - М.: Феникс, 2017. – 60 с.
8. Бернет М., Клейман Д. Как создать свой идеальный пароль. Выбираем пароли, отпугивающие хакеров. - М.: НТ Пресс, 2019. – 176 с.
9. Жуков Ю.В. Основы веб-хакинга. Нападение и защита. - М.: Питер, 2018. – 208 с.
10. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей. // Журнал «Информационная безопасность». - № 5. 2013. – С. 15.
11. TECHNOLOGY TRANSFER IN DIGITAL ERA: LEGAL ENVIRONMENT Bliznets I., Kartskhiya A., Smirnov M. - Tarih Kültür ve Sanat Araştırmaları. 2018. Т. 7. № 1. С. 354-363.
12. Фленов М. Компьютер глазами хакера. - М.: «БХВ-Петербург», 2019. –336 с.

Оригинальность 85%