Федеральное агентство по образованию

Московский Государственный Университет
Приборостроения и Информатики

Кафедра «Философия»

РЕФЕРАТ

для сдачи кандидатского экзамена
«История и философия науки»

Тема: «Информационная безопасность – история проблемы и ее решение»

Аспирант 1 года обучения
Каф. ИТ-2 спец. 010204
Либкинд Артем Сергеевич
29.03.2009

Допускается
Зуев Владимир Васильевич
д.ф.-м.н.,проф.

Оценка
Преподаватель
уч. степень _____ уч. звание _____
Подпись
Дата

Москва 2009

Оглавление

Введение

Информационная безопасность в современном обществе - одна из самых больших проблем как для организаций, так и для конечных пользователей. Однако в то время, как конечные пользователи не уделяют ей должного внимания, а зачастую даже пренебрегают простейшими рекомендациями по безопасности, в организациях для защиты корпоративной информации выделяются немалые материальные средства и человеческие ресурсы. Согласно ГОСТу РФ[1], информационная безопасность — защита конфиденциальности, целостности и доступности информации. Однако проблема безопасности информации — не проблема современного времени, люди древних времен испытывали те же проблемы. Наши предки, скорее всего, не задумывались над терминологией, но так же хотели, чтоб их письма не были прочитаны никем, кроме адресата, дошли до места назначения целыми, и не были бы подделаны недоброжелателями. Но если в те времена это касалось только важных господ и власть имущих, то сейчас это касается каждого пользователя Интернета. И если кража корпоративной информации может привести к потере прибыли или разработки, то подделка или утечка личной переписки может привести к разрушению вполне счастливой семьи или распаду дружного коллектива. Если рассматривать информационную безопасность в том виде, в котором этим понятием оперируем мы сейчас, то речь конечно же идет о информации хранящейся или передающейся с помощью современных технических средств, а в первую очередь с помощью компьютеров.

Так же хотелось бы отметить такое определение информационной безопасности, которое дает «Рекомендация по стандартизации информационных технологий»[2]: безопасность информации — состояние защищенности информационной технологии, обеспечивающее безопасность информации, для обработки которой она применяется, и информационную безопасность автоматизированной информационной системы, в которой она реализована. Если более подробно рассмотреть это определение, то становится понятно, что информационная безопасность призвана обеспечить надежность не только информации, но и системы, в которой она хранится и работает. В современных организациях эту функцию берут на себя системные администраторы, которые в большинстве случаев так же занимаются проблемами безопасности и сохранности и существующей информационной инфраструктуры, и защитой самих данных.

В своей работе я планирую осветить исторические аспекты возникновения проблемы информационной безопасности, разные градации современного вида данной проблемы, а так же рассказать об основных направлениях решений проблемы.

Исторические аспекты возникновения и развития информационной безопасности

Хронология

По мнению Лопатина В. Н.[3], объективно категория «информационная безопасность» возникла с появлением средств информационных коммуникаций между людьми, а также с осознанием человеком наличия у людей и их сообществ интересов, которым может быть нанесен ущерб путем воздействия на средства информационных коммуникаций, наличие и развитие которых обеспечивает информационный обмен между всеми элементами социума. Учитывая влияние на трансформацию идей информационной безопасности, в развитии средств информационных коммуникаций можно выделить несколько этапов:

- I этап — до 1816 года — характеризуется использованием естественно возникавших средств информационных коммуникаций. В этот период основная задача информационной безопасности заключалась в защите сведений о событиях, фактах, имуществе, местонахождении и других данных, имеющих для человека лично или сообщества, к которому он принадлежал, жизненное значение.
- II этап — начиная с 1816 года — связан с началом использования искусственно создаваемых технических средств электро- и радиосвязи. Для обеспечения скрытности и помехозащищенности радиосвязи необходимо было использовать опыт первого периода информационной безопасности на более высоком технологическом уровне, а именно применение помехоустойчивого кодирования сообщения (сигнала) с последующим декодированием принятого сообщения (сигнала).
- III этап — начиная с 1935 года — связан с появлением радиолокационных и гидроакустических средств. Основным способом обеспечения информационной безопасности в этот период было сочетание организационных и технических мер, направленных на повышение защищенности радиолокационных средств от воздействия на их приемные устройства активными маскирующими и пассивными имитирующими радиоэлектронными помехами.
- IV этап — начиная с 1946 года — связан с изобретением и внедрением в практическую деятельность электронно-вычислительных машин (компьютеров). Задачи информационной безопасности решались, в основном, методами и способами ограничения физического доступа к оборудованию средств добывания, переработки и передачи информации.
- V этап — начиная с 1965 года — обусловлен созданием и развитием локальных информационно-коммуникационных сетей. Задачи информационной безопасности также решались, в основном, методами и способами физической защиты средств добывания, переработки и передачи информации, объединенных в локальную сеть путем администрирования и управления доступом к сетевым ресурсам.
- VI этап — начиная с 1973 года — связан с использованием сверхмобильных коммуникационных устройств с широким спектром задач. Угрозы информационной безопасности стали гораздо серьезнее. Для обеспечения информационной безопасности в компьютерных системах с беспроводными сетями передачи данных потребовалась разработка новых критериев безопасности. Образовались сообщества людей — хакеров, ставящих своей целью нанесение ущерба информационной безопасности отдельных пользователей, организаций и целых стран.

Информационный ресурс стал важнейшим ресурсом государства, а обеспечение его безопасности — важнейшей и обязательной составляющей национальной безопасности. Формируется информационное право — новая отрасль международной правовой системы.

- VII этап — начиная с 1985 года — связан с созданием и развитием глобальных информационно-коммуникационных сетей с использованием космических средств обеспечения. Можно предположить, что очередной этап развития информационной безопасности, очевидно, будет связан с широким использованием сверхмобильных коммуникационных устройств с широким спектром задач и глобальным охватом в пространстве и времени, обеспечиваемым космическими информационно-коммуникационными системами. Для решения задач информационной безопасности на этом этапе необходимо создание макросистемы информационной безопасности человечества под эгидой ведущих международных форумов.

Описание этапов развития информационной безопасности

Мы можем легко перечислить все методы защиты информации, разработанные на первом этапе её развития: подписи, личные печати, ручная и механическая шифрация, сокрытие факта передачи информации. Несмотря на простоту многих методов шифрации тех времен, они выполняли свою главную задачу — неприятель не мог получить информацию в короткий срок, даже перехватив само сообщение. Время, необходимое на расшифровку закодированного сообщения, почти всегда делало информацию неактуальной. Основой любого шифра во все времена являлся ключ шифрации, который в те времена был самой интересной частью любого алгоритма шифрации. Пронумерованные листочки, с прорезанными «окошками», которые надо было поворачивать поверх сообщения, и читать получающиеся слова в окошках, или знаменитые «пляшущие человечки» из рассказов Конан Дойля, которые имеют под собой вполне реальную основу. Еще стоит упомянуть такую методику шифрации сообщений, как «письмо в письме», популярную и в наше время. Смысл этой методики состоял в том, что внутри письма на заурядную тему о погоде или о здоровье родственников, по определенному принципу (подстановка слов, ключевые фразы) содержалась информация о важных вещах, например о времени и месте тайной встречи или донесения разведки о передвижении сил неприятеля. Первым известным средством защиты информации считается древнегреческая скитала, описание которой было дано в 120 году до н.э. Она работала по следующему принципу: у отправителя и адресата были палки одинаковой толщины. Отправитель наматывал на палку тонкую полоску папируса, и писал по горизонтали буквы. После разворачивания папируса получалась беспорядочная последовательность букв, прочитать которую можно было лишь с помощью палки такой же ширины. Самым уязвимым местом этого этапа становится человеческий фактор, в виде ненадежных посланников и потенциальных изменников из тех, кто знает секрет кода. Здесь и далее, под термином «человеческий фактор» мы будем понимать устойчивое выражение, которым обозначают психические способности человека как потенциальный и актуальный источник (причину) информационных проблем (коллизий) при использовании этим человеком современных технологий.

Второй временной этап ознаменовался появление в широком употреблении телеграфов и подобных им устройств. К классическим проблемам защиты информации добавилась очень интересная концепция — заинтересованный в информации человек мог «подключиться» к линии передачи информации, и слушать всю проходящую информацию. А с учетом единого принятого в мире языка телеграфов — азбуки Морзе, для прослушивания передаваемой информации не было никаких препятствий. Еще на пути тех,

кто хотел сохранить свою информации в целости встала другая проблема, на этот раз технического характера — информация порой могла дойти не вся или дойти с определенными ошибками. Как результат, обычные телеграфный аппарат военного образца содержал в себе автоматический механический модуль, шифровавший информацию по определенному образцу, а так же генератор «белого шума» - набора помех, забивавшего линии передач все время, пока не происходило передачи информации. Как результат, потенциальный неприятель не могу узнать, когда начинается и заканчивается настоящая передача. Так же стало проще подделывать письма, переданные с помощью телеграфа, ведь теперь в них не использовался почерк и печать, а текст сообщений весьма сократился, ведь каждая буква стоила денег. Самым уязвимым местом на этом этапе продолжает оставаться человеческий фактор, но теперь это уже фактор людей, связанных с «программированием» шифрующих модулей.

Третий временной этап дал восхитительную технологию для передачи информации — радио. Длинные и короткие волны не зависят от проводов, и покрывают немалые расстояния, но любой настроенный приемник в зоне вещания может получить и воспроизвести передаваемую информацию. Для защиты информации использовались почти те же самые технологии, что и во времена телеграфов, но более сложные в технологическим плане. В большинстве мест белый шум был заменен на непрерывную трансляцию какой-либо статистической информации, при прерывании которой вещающая точка должна была выйти на связь и подтвердить, что это тот же самый источник. Другой вариант подразумевал сохранения полной тишины в эфире, а при сеансах связи, происходивших в заранее определенное время, передаваемый сигнал модулировался белым шумом, и для стороннего слушателя от шума и не отличался. Стоит отметить, что подделка радиопередачи намного сложнее подделки телеграфного сообщения, ведь через радиоканал передается голос, да и длина время передачи не так ограничено. К общему набору уязвимых мест добавилась возможность перехвата оборудования, изучение которого могло дать неприятелю ключ ко всем предыдущим передачам.

Четвертый этап поставил точку на шифрах, основанных на подмене символов. Большие, громоздкие компьютеры, которые могли делать по несколько сотен математических операций в секунду, раскрывали такие шифры в весьма короткие сроки. Намного сложнее компьютерам было совладать с радиограммами, ведь вся информация для компьютера состоит из единиц и нулей, перевести в которые звук не так просто. Из-за размеров самих компьютеров для генерации шифров они не использовались. По сравнению с третьим этапом, в самой методике шифрации и защиты информации ничего не изменилось, так же не изменились уязвимые места систем.

Пятый этап начался с прорыва в области коммуникаций — парой нажатий клавиш любой желающий может получить научную статью, исходный код программы или другую полезную информацию. Компьютеры объединяются в локальные сети, специалисты фантазируют о сетях, которыми будет опутан весь мир, и пользователя ПК из Англии будет отделять от пользователя ПК из Америки или Китая лишь пара нажатий клавиш. Пока же лишь внутри крупных университетов, а так же в ряде военных учреждений введены локальные компьютерные сети, но уже тогда начинают разрабатываться системы противодействия потенциальным похитителям информации, ведь сама логика работы локальной сети подразумевает доступной общей информации из любой точки. В это же время впервые, применительно к компьютерам, используется термин «парольной защиты» - некоего кода, с помощью которого пользователь может получить доступ к данным и к компьютеру вообще. В это время начинают закладываться основы информационной безопасности в том виде, какой мы знаем ее сейчас. Основной уязвимостью становится человеческий фактор — невнимательный или неблагонадежный сотрудник может совершить

ошибку, которая даст потенциальному злоумышленнику доступ к информации.

Шестой этап, по мнению Лопатина В. Н., ознаменовался появлением «хакеров», а так же мобильных рабочих станций. Однако, если быть точными, «хакер» как термин появился приблизительно в 1960 году, в Массачусетсском технологическом институте, где этот термин использовался для обозначения любого программиста, придумавшего либо очень необычное и хитрое решение, либо очень грубое, но эффективное. Весьма быстро этот термин стал означать любого компьютерного специалиста. Что касается информационного права и безопасности информации государства, то это относиться лишь к очень маленькому числу стран, а так же не следует забывать о том, что многие важные информационные структуры остаются изолированными от внешнего доступа. В это же время как раз формируются основные рекомендации по защите информации и безопасной работе на персональных компьютерах. Персонал, которому доверялись персональные компьютеры для работы на них дома, обязательно должен был пройти аттестацию на умение работать на ПК, а так же обязался не оставлять не заблокированный компьютер без внимания, не использовать простых паролей и не давать физического доступа к самому компьютеру. В это же время компания IBM выходит на рынок с революционным решением — открытая архитектура. До этого момента все компьютеры были моноблочны — они поставлялись как готовое изделие, и не подразумевали каких либо изменений в своей структуре. Конечно, всегда находились умельцы, но таких было очень мало. IBM предложили выпускать отдельные компоненты, чтоб каждый желающий смог собрать такой компьютер, какой ему нравится и подходит для его задач. Пару лет спустя появляются модули для аппаратной защиты данных — отдельные платы, при использовании которых физически на жестком диске информация хранится в зашифрованном виде, и без знания пароля не может быть оттуда считана. При этом система полностью прозрачна для пользователя, ведь любые сделанные изменения уже записываются на диск как зашифрованная информация. Вторым вариантом криптозащиты являются программные решения, которые требуют при начале работы с данными расшифровать их, а после работы зашифровать. В случае с программной защитой, может быть немало вариантов, при которых конечная шифрация не будет выполнена и информация будет легко доступна. Самой страшной уязвимостью остается человеческий фактор — многие люди считают излишним использовать пароли или оставляют их слишком простыми. Появляются уязвимости, связанные с ошибками в программном обеспечении, при которых некорректная работа программы может привести к потенциальной потере данных.

Седьмой этап, киберсеть в том виде, какой мы знаем ее сейчас, самой большой из которых является Интернет. Множество людей каждый день используют сеть, не задумываясь о личной безопасности. Ошеломляющее количество компьютеров, без ведома их владельцев объединяются в единое логическое пространство, чтоб устраивать атаки на сайты, рассылать нежелательную почту или захватывать другие сегменты сети. Такими компьютерами, как правило, манипулирует один человек, написавший сложный вирус. Даже самые маленькие организации не представляют себе работы без нескольких персональных компьютеров, объединенных в отдельную сеть. Колоссальные суммы денег и объемы человеческой работы служат для создания систем защит для конечных пользователей. Сегментов сети и даже самого интернета. Резко меняется ценность информации — огромное количество личной, конфиденциальной переписки каждый день пересылается через незащищенные сети, использование слабых паролей дает злоумышленникам возможность получать доступ к огромному количеству информации, а методики обучения людей работе на ПК даже не подразумевают минимального обучения защите в информационной среде.

Вот так, с древних времен до наших дней складывалось понятие информационной безопасности. Чем сложнее становилась техника, чем больше доверялось ей информации,

тем сильнее была необходимость сохранять ее в целости и сохранности. Последнее время так же требуется, чтоб сохранна была не только информация, но и сама инфраструктура организаций, обеспечивающая доступ и безопасность.

Современные угрозы безопасности

Информационной безопасности не было бы, если бы не было информационной опасности. Если быть точными, то безопасных мест для информации нет, но это очень пессимистический подход. Самих информационных угроз великое множество, но если разбить их на категории, то мы получим примерно следующую классификацию:

- утечка информации,
- повреждение информации,
- нелегальное использование информационного носителя,
- повреждение системы хранения информации.

В наше время людей, которые воруют информацию принято называть «хакерами», или в дословном переводе «взломщиками».

Хакеры

Как было сказано выше, этот термин возник в 1960 году, и означает «компьютерный специалист». Основной работой хакеров тех лет было создание «хаков» - маленьких заплаток, исправляющих некорректную работу программ других авторов. Более всего ценилось умение делать такие заплатки на лету, сразу указывая автору, где у него ошибка и предлагая готовый вариант решения. Но не все, работавшие таким образов, делали это из благих побуждений. Заплатка, исправляющая неправильный подсчет в программе для статистики, могла отсылать автору заплатки копию данных, или даже полностью портить программу и компьютер автора начальной программы. Такие случаи сразу становились достоянием прессы, как и указание на то, что это было сделано тем или иным хакером. Вокруг хакеров стала складываться дурная слава, а понимание хакерства как активной обратной связи между авторами и пользователями программ, к сожалению, ускользнуло от внимания журналистов. В результате появилось новое, искажённое понимание слова «хакер», означающее злоумышленника, использующего обширные компьютерные знания для осуществления несанкционированных, иногда вредоносных действий с компьютерами - взлом компьютеров, написание и распространение компьютерных вирусов. Впервые в этом значении слово «хакер» было употреблено Клиффордом Столлом в его книге «Яйцо кукушки», а его популяризации немало способствовал голливудский кинофильм «Хакеры». В подобном компьютерном сленге слова «хак», «хакать» обычно относятся ко взлому защиты компьютерных сетей, веб-серверов и тому подобному.

Культура современных хакеров построена на принципе «Information must be free», что переводится как «Информация должна быть свободной». Большей частью, действия всех известных хак-групп направлены на борьбу с коммерческим ПО, сокрытием информации и неправильным использованием технологий. Они взламывают программы, делая для всех желающих маленькие заплатки, с помощью которых можно пользоваться платной программой бесплатно, воруют серийные номера от операционных систем, раздавая желающим, выкрадывают из организаций базы данных и кладут на всеобщее обозрение. По своей сути они ведут информационную войну. Какого-то четкого принципа, центра и метода у них нет — можно сказать, что, сколько хакеров, столько и мнений. А общее количество

пользователей интернета и всеобщая анонимность делает их неуловимыми для правоохранительных органов стран мира, и только из-за радикальных ошибок обычно удается поймать кибер-преступника.

Самым известным в мире хакером считается Кевин Митник, в «заслугах» которого даже числится взлом Пентагона. Кевин открыто продемонстрировал, что самой уязвимой частью любой компьютерной системы является человек, ведь «проще всего попасть в дом, не сломав дверь, а попросив ее открыть». Однако в 1995 году он был арестован и осужден на 2,5 года тюремного заключения, ввиду того, что многие из его «злодеяний» недоказуемы. По истечении срока ареста Кевину поныне запрещено пользоваться компьютерами, интернетом и сотовыми телефонами.

Нередко хакеры взламывают веб сайты или системы лишь затем, чтобы продемонстрировать их владельцам слабые места. Нередко таки случаи вызывают немалый ажиотаж среди мирного населения. Последним подобным инцидентом стал взлом системы управления и наблюдения за большим адронным коллайдером, когда группа римских хакеров получила доступ к основным показателям счетчиков. Ничего ломать и портить хакеры не стали, а лишь указали администрации на ошибки, но СМИ не поленились заметить, что они могли бы изменить какие нибудь коэффициенты, что могло бы привести к весьма плачевным результатам.

Вирусы

Я не буду углубляться в классификацию различных видов вредоносного ПО, отнеся подобные программы к единой категории «вирусы». Происхождение этого термина, применительно в компьютерному ПО неслучайно. Я позволю себе процитировать учебное пособие В. А. Каймина[6]: «*Компьютерный вирус был назван по аналогии с вирусами биологическими. По всей видимости, впервые слово вирус по отношению к программе было употреблено Грегори Бенфордом (Gregory Benford) в фантастическом рассказе «Человек в шрамах» (The Scarred Man), опубликованном в журнале Venture в мае 1970 года. Термин «компьютерный вирус» впоследствии не раз открывался и переоткрывался — так, переменная в программе PERVADE (1975), от значения которой зависело, будет ли программа ANIMAL распространяться по диску, называлась VIRUS. Также, вирусом назвал свои программы Джо Деллинджер (англ. Joe Dellinger), и, вероятно, — это и был первый вирус, названный собственно «вирусом».*

Несколько лет назад, основной целью работы компьютерных вирусов был вывод из строя ПК пользователя, уничтожение его информации, приведение компьютера к состоянию, в котором работать с ним становилось невозможно. Когда интернет стал более широко распространен, появились программы для перехвата управления компьютером, возможно даже и без ведома пользователя. Не менее популярны сейчас программы, ворующие пароли от почты, сайтов, форумов, перехватывающие данных для интернет платежей, в результате чего злоумышленник «влезает» в кошелек жертвы. И самые жестокие вирусы, которые незаметно для пользователя «подчиняют» его компьютер одному человеку, прибавляют его к единой сети, которые начинают рассылать нежелательную почту, взламывать сервера или просто перебирать пароли. Последняя такая эпидемия затронула 6,5 миллионов компьютеров.

Существуют также вирусы, которые портят аппаратную часть компьютера. Самым известным таким вирусом является «Чернобыль», который активизируется каждое 26 апреля в году, уничтожая файлы и пытаясь испортить базовую систему ввода-вывода компьютера, что приводит к необходимости замены немалого количества комплектующих. Данный вирус работает только под старыми операционными системами Windows версий 95

и 98, и не опасен в наши дни.

Зачем делают вирусы? Основных причин для создания зловредных программ всего три — деньги, популярность, желание самосовершенствования. Вирус, ворующий пароли от интернет-кошельков, или объединяющий компьютеры в сеть и рассылающий нежелательную почту, может принести своему разработчику немалую прибыль. Так же как и авторы самых серьезных разновидностей вирусов становятся весьма популярны в определенных кругах, и нередко получают предложения о хорошей работе в крупных компаниях. Ну и всегда создателям вирусов интересно первыми найти критическую ошибку разработчиков и продемонстрировать всем, насколько совершенно они могут такой уязвимостью воспользоваться.

Почему вирусы существуют? Сама организация современных операционных систем подразумевает существование вирусов. В настоящий момент, в основном в мире используется две, полностью различные между собой, операционные системы — Windows и Linux. Правильная маркетинговая политика в течении почти двух десятков лет обеспечила Windows абсолютно прочное место на рынке. Но за такую роскошь приходится платить — из чего на самом деле состоит эта система, и где в ней потенциальные опасности не знает никто. Какую-то часть знают разработчики, но они не спешат делиться этой информацией, а сама система очень активно сопротивляется любым попыткам отследить ее активность. Как результат, компьютерные специалисты «на ощупь» пытаются разобраться в ее устройстве, в результате чего потихоньку они находят в ее устройстве ошибки, которые и используют для создания вирусов. Разработчики системы сразу же выпускают заплатку, исправляющую ошибку, как результат, разработчики могут лишь дать гарантию, что «второй раз от той же проблемы ваши данные не будут украдены». Но есть маленькая проблема. Операционная система стоит достаточно дорого. Поэтому многие пользователи пользуются ворованными взломанными её копиями, которые не могут получать эти обновления. Хотя если посмотреть комплексно, то при использовании лицензионной системы, хорошего антивирусного программного обеспечения и соблюдении техники безопасности при работе в Интернет, шанс оказаться жертвой вируса минимален. К сожалению, критичным фактором в этом наборе является соблюдение техники безопасности, потому что в обратном случае ни обновления системы, ни защита не помогут.

Другая операционная система, Linux, начинала разрабатываться как раз теми самыми «хакерами», когда этот термин еще означал специалистов. Она основана на открытом исходном коде. Это означает, что любой, кому это будет интересно, может всегда посмотреть, каким образом устроен каждый модуль его системы. Есть группа разработчиков, которые делают «скелет» системы — ядро, а так же огромное количество независимых пользователей, разрабатывающих сторонние программы. Основным принципом всех программ является их доступность и открытость исходного кода. В результате сложилось огромное сообщество, которое перекрестно проверяет работу друг друга, подсказывая авторам, где содержатся ошибки и как их лучше исправить. При работе в этой операционной системы пользователю не следует опасаться вирусов, которые смогут пробраться через ошибки операционной системы, такие вирусы бесполезно разрабатывать, ведь исправление от ошибки будет создано уже в тот же день, и в течение еще пары дней подавляющее количество пользователей установят себе это обновление. К сожалению, не все так хорошо в этой системе — и основная причина тут деньги. Система бесплатна, программы под нее тоже бесплатны, поэтому она была и остается системой для специалистов. Человеку, плохо разбирающемуся в современных информационных технологиях скорее всего не удаться установить и настроить себе систему до полной функциональности. Так же, программы для обоих систем несовместимы между собой. С большим количеством «но» можно запустить программы для Windows под Linux, но работать они, скорее всего, будут «немного не так».

Человеческий фактор

Для обеих систем самой страшной уязвимостью является человеческий фактор. Самая страшная вещь, с которой сталкивается любой специалист по информационной безопасности состоит в том, что когда пользователь видит надпись «нажмите Да чтоб отправить нам все ваши пароли и увидеть красивую картинку», он нажимает да. Здесь работает социология и психология, заставляя пользователей все-таки отдать свои пароли и личную информацию, хотя если пользователя честно спросить поступил бы он так, пользователь говорит «конечно же, нет!».

Помимо очевидных глупостей при работе в сети, пользователи очень часто не могу запомнить сложных паролей. Как результат они или используют простые пароли, например, дату рождения, домашний телефон или просто комбинации «123456», или держат свои пароли записанными на бумажках, приклеенных к монитору. А если хакер хочет собрать определенную информацию с компьютера жертвы, ему вполне хватит минуты времени, чтоб обеспечить себе спокойный и безопасный доступ из любого места к компьютеру жертвы — надо лишь сесть один раз за ее компьютер, ввести пароль и воткнуть флешку.

Также в последнее время стал популярным следующий способ обмана: пользователь получает на почту программу, замаскированную под картинку или документ с примечанием: «посмотри какая классная фотография» или «вот запрошенные вами документы». Пользователи скачивают приложение к письму и честно запускают. После этого у хакера в распоряжении свободный доступ к компьютеру. Все современные сервисы, предоставляющие людям почту, предупреждают «не открывайте письма, адресованные не вам!», но мало кто к ним по-настоящему прислушивается.

Не стоит забывать, что у каждого есть свои слабости и страхи. Если злоумышленники решили выудить информацию из конкретного человека, они не стесняются использовать такие методы как запугивание и шантаж. Таким атакам нередко подвергаются администраторы крупных систем, которые защищены достаточно серьезно и находятся под круглосуточным наблюдением. В наше время, благодаря разным информационным источникам, нетрудно узнать почти о любом человеке немало подробностей, чтоб получить рычаги давления. А запугивать человека можно целиком информационными средствами, и просто дождаться, пока он совершит ошибку или у него сдадут нервы. Так же, нередко администраторы совершают ту же ошибку, откликаясь на предложения «фальшивых» писем.

Поддельный интернет

Со времен телеграфов, злоумышленники врезались в линии передач, прослушивали и меняли содержимое сообщений, передаваемое по проводам. В наше время, конечно, достаточно сложно подключиться к проводам, но вот бесплатный интернет в общественных местах довольно часто оказывается подделкой. Все, что работает через такое подключение, записывается на определенный носитель. В дальнейшем его владелец может получить оттуда пароли, ключи от интернет кошельков и всю проведенную переписку. Но что еще страшнее — программы любят автоматически обновляться, увидев доступ в интернет. Антивирусы, система, клиентское ПО зачастую само скачивает файлы для себя и инсталлирует. Злоумышленник вполне может подменить заранее эти файлы на содержащие необходимые ему заплатки. Проблеме получения «поддельных» обновлений посвящено немало усилий разработчиков, и к их чести следует заметить, что на самом деле для серьезных продуктов шанс получения таких обновлений минимален.

В современном мире большинство пользователей не знают, как устроен интернет.

Для пользователя все просто — он набирает в строке браузера адрес и попадает на интересующую его страницу. Сколько точек и сервисов при этом задействовано для выполнения этого вызова, пользователя не интересует. Поэтому пользователи порой попадаются на фальшивые ссылки, не видя существенной разницы между www.yandex.ru и wwvv.yandex.ru. Фальшивые ссылки никогда не приводят ни к чему хорошему, поэтому очень полезно внимательно смотреть, куда вы собираетесь перейти с текущей страницы. Так же, пользователи редко не интересуются, по какому пути идет их трафик, не перехватывает ли его кто-нибудь.

Фальсификация информации

Данные, передаваемые компьютерами, состоят из нулей и единиц. Любая последовательность данных может быть заменена на другую или сфабрикована. Большинство современных каналов радио, телефонной и видео связи цифровые, и передают информацию в том же формате. Получатель может получить неверные данные, или даже информацию, которую настоящий отправитель не посылал. Нередко злоумышленники взламывают веб сайты организаций, меняя содержимое страниц на порочащую организацию информацию.

Другую проблему представляют сотрудники организаций, которые пишут в личных блогах (веб дневниках, ставшими популярными в последнее время) нелицеприятную информацию о своем месте работы. Организации, для которых важно мнение пользователей сети, или работа которых напрямую зависит от интернета, постоянно отслеживают упоминания о себе, а так же следят за дневниками сотрудников. Нередки случаи увольнения сотрудников за порочащие организацию записи.

Нередко записи в дневниках людей приводят к неожиданным последствиям. Администрация ресурсов, предоставляющих пользователям возможность вести онлайн дневники, требует соблюдать федеральные законы, и не выкладывать материалов, противоречащих законодательству, но порой грань бывает очень тонка.

Автор одного из дневников, после рассказов СМИ о стрельбе в одном из американских учебных заведений, написал рассказ, в котором повествование велось от лица террориста, а местом действия было одно из уральских политехнических учебных заведений. Этот рассказ увидел сотрудник МВД, и автору было предъявлено обвинение "заведомо ложное сообщение об акте терроризма". Было произведено несколько экспертиз, и в результате автор был осужден на два года условного заключения.

Другой случай, произошедший так же в России, стал первым случаем обвинения человека за его запись в электронном дневнике. В этой записи автор рассказал о своем отношении к сотрудникам милиции, которые, по его мнению, отнеслись к нему весьма несправедливо и негуманно. Автор понес наказание в виде года условного заключения.

Нередко манипуляции с информацией приводят к более масштабным последствиям. Вспомним недавний Иракский конфликт, в ходе которого имела место крупная фальсификация отчетов экспертов, приведшая к введению войск в мирные города, в результате чего назвать произошедшее иначе, чем войной, тяжело.

Утечка информации

Информация должна быть доступна пользователю, это одно из требований информационной безопасности. Но если конфиденциальную информацию получит злоумышленник и передаст ее заинтересованным лицам, оригинальный обладатель

информации может оказаться в очень неприятном положении. Это может оказаться база данных клиентов, с помощью которой конкурирующая фирма сможет перетянуть клиентов, или секретные правительственные данные, которые могут привести к войне. В наше время информация становится основным ресурсом, и доступ к информации сторонних людей может привести к необратимым последствиям. Информация становится ценной, если она востребована. Школьник может найти в интернете рецепт создания бомбы, или чья-то личная переписка может стать причиной развода. Нередко крупные организации оказываются объектами шантажа со стороны злоумышленников, получивших доступ к личным данным сотрудников или выкравшим базы бухгалтерии. А похищение правительственных данных с последующей передачей данных правительствам других стран может стать причиной резкого обострения международной обстановки.

Пираты

Как только появилась возможность прослушать музыку и просмотреть фильм на компьютере, пользователи начали делиться подобной информацией друг с другом. Изначальные правообладатели оказались перед ситуацией, когда колоссальные объемы музыки и фильмов передаются между пользователями абсолютно бесплатно. Суммы, которые звукозаписывающие компании называют своими убытками от действий «пиратов», поражают воображение. С пиратством в сети ведется самая настоящая война, но до сих пор эффект такой борьбы весьма мал. Кино, вышедшее в кинотеатрах, на следующий день уже можно найти в сети. Музыка весьма часто попадает на всеобщее обозрение еще до своего выхода в свет. Множество людей занимается оцифровкой книг с последующим распространением.

С другой стороны, распространение информации через интернет имеет множество положительных сторон. Для молодых авторов это удобный способ заявить о себе, нередко на определенных сайтах образуются прекрасные научные библиотеки, где все желающие могут найти редкие, почти недоступные издания научных книг.

Во многих странах сегодня за свободное распространение информации, защищенной авторским правом, предусмотрена уголовная ответственность, но подавляющая анонимность пользователей сети служит неплохой защитой от уголовного преследования.

Информационная безопасность: методы защиты

Угроз личной информации, как и самому компьютеру на сегодняшний день более, чем достаточно. Множество людей каждый день пишут новые модификации вирусов, ищут ошибки в программном обеспечении или исследуют сайты на предмет ошибок. Не меньшее количество людей каждый день дорабатывает уже текущие методы защиты, а так же выпускает новые.

Структура

Информационная безопасность предъявляет к любому средству защиты три основных требования — конфиденциальность, целостность, доступность. Более широко, к информации должны получить доступ только те, кому она предназначена, информация должна быть доступна в полном объеме, и информация должна быть доступна пользователю при необходимости.

Антивирусы

Самым простым и доступным методом защиты для пользователя является антивирусное программное обеспечение, или просто антивирус. Антивирус служит для защиты от всех угроз, которые могут коснуться пользователя.

Виды антивирусов, а так же их области применения весьма различны. В общем случае антивирус проверяет все вновь попадающие на компьютер файлы, а так же отслеживает их активность во время работы. Так же к антивирусам можно отнести межсетевые экраны, которые контролируют активность всех работающих в сети программ, блокируя нежелательную для пользователя активность.

Основным недостатком антивирусов является сама основа их работы — они выполняют защитную функцию. Проверка файлов и контроль активности производится по заранее известным шаблонам, и принципиально новую версию вируса антивирусы почти никогда не могут остановить. Конечно, самые серьезные из современных антивирусов оснащены так называемой «эвристической защитой», которая должна по общим симптомам активности программы определить, не является ли она вредоносной, но и эта линия защиты далека от совершенства — компьютер не может точно определить какое приложение полезно пользователю, а какое нет.

Организация сети

Другим уровнем защиты пользователей является сама система организации современного интернета. Весь интернет поделен на зоны, в большинстве случаев совпадающими с границами стран, и эти зоны «общаются» друг с другом через дорогое, специализированное оборудование. Операторы такого оборудования находятся в непрерывной коммуникации между собой, и при появлении вирусной активности в одной из зон, операторы остальных зон пытаются изолировать свои зоны от специфической вирусной активности. К сожалению, это помогает защитить пользователей лишь от механизма распространения вирусов, заложенного в самих вирусах.

В некоторых странах правительство пришло к решению контролировать весь сетевой трафик жителей. В большинстве случаев это сводит на нет любую анонимность в сети, но так же весьма повышает защищенность веб страниц и почты от возможности пересылки вредоносных программ.

Непрерывное наблюдение

Более локальным уровнем защиты информации является контроль сотрудниками отдела информационных технологий или отдела безопасности организация действий пользователей. В зависимости от правил конкретной организации, может контролироваться любая активность пользователя, включая просмотр всей почты и посещения сайтов, или лишь общий факт получения доступа к информации.

На государственном уровне есть специальные органы, которые следят за общением людей в интернете, сообщениями на форумах, появляющейся в СМИ новостях. В случае нарушения определенных законов, ил если по мнению представителей органов выложенная информация может быть опасна, она немедленно убирается.

Электронная подпись

Для достоверности переписки было создана система электронных подписей, которая гарантирует получателю, что письмо отправлено настоящим отправителем. Все используемые на сегодняшний день системы электронных подписей полностью исключают возможность подделки такой подписи. Единственной угрозой безопасности такого метода является компрометация подписи, которая подразумевает, что к исходным файлам подписи получил доступ сторонний человек.

К сожалению, применение системы электронных подписей требует определенной инфраструктуры, и пользователи очень редко используют подобную переписку ввиду общей сложности применения метода. Однако вся конфиденциально важная переписка организаций с налоговыми органами, а так же банками обязательно защищается подобным методом.

Шифрация

Зашифрованные данные представляют из себя полную бессмыслицу, для человека не владеющего кодом и алгоритмом шифрации. Современные возможности компьютеров выдвигают весьма высокие требования к механизмам шифрации, и даже при соблюдение этих требований не дает гарантии полной защиты. Основной закон криптографии гласит «Стойким считается алгоритм, который для успешной атаки требует от противника недостижимых вычислительных ресурсов или же такого времени раскрытия, что по его истечению защищенная информация будет уже не актуальна», то есть потенциально любая системы может быть взломана, все зависит лишь от срока и затраченных ресурсов.

Информационная безопасность: предотвращение угроз

Источник угрозы

В общем случае, проблемы информационной безопасности связанны с мировоззрением конкретных людей, которых не устраивает текущая ситуация. Это могут быть сотрудники, которые готовятся к увольнению, и пытающиеся забрать с собой базу клиентов, просто чтобы навредить напоследок, или хакер, который считает что разработчики конкретной программы требуют за нее большие деньги, но делают свою работу плохо. Мотивация компьютерного пиратства недалека от причин пиратства морского — зачем платить за что то, когда это можно получить бесплатно? В большинстве случаев, люди делают в сети противозаконные вещи, просто потому, что не ассоциируют их с реальной жизнью. Есть правила, установленные обществом, религией, государством — не убий, не укради, не сквернословь. На самом деле установка взломанной программы ничем не отличается от кражи шоколадки из магазина. Как и скачивание фильма является кражей у его правообладателя. Меньшая часть людей может аргументировать свою правоту в этом вопросе, и все же их доводы не отличаются от доводов обычных преступников. Большая же часть людей совершает эти преступления, не задумываясь, что это вообще плохо.

Те же, кто ведет в сети войну с корпорациями, с тотальным контролем интернета, придумывают методы обмана средств наблюдения, ничем принципиально не отличаются от анархистов. Из девизы и метод действия во многом восходит к описанному в книге Уильяма Пауэлла «Поваренная книга анархиста», которая в определенных кругах считается культовой.

Самое страшное, что сама среда толкает людей на такой образ деятельности. Человек, использующий интернет перестает быть собой. В интернете у него может быть другое имя, там он может быть кем угодно. И очень непросто связать реального человека с его альтер-эго из интернета, что дает человеку несказанное чувство свободы и независимости. В интернете нет законодательной и исполнительной власти, и наказание за преступления не будет. При этом человек, скорее всего, даже не задумывается никогда об этом, но он это чувствует и позволяет себе вести себя соответствующим образом.

Напрашивается грустный вывод — если в средние века угрозу информационной безопасности представляли единичные индивидуумы, которые считали нормальным подделывать информацию или позволяли себе узнавать чужие тайны, то и сейчас люди, причастные к краже и подделке информации, делают это в согласии со своей моралью и этикой. Можно долго обсуждать, имеет ли право менеджер при увольнении забрать с собой базу клиентов, но факт незаконной установки программного обеспечения интерпретировать иначе, нежели преступление тяжело.

Фальсификация информации СМИ так же имеет под собой моральную проблему — желание славы и популярности. Немало журналистов готовы во имя собственного честолюбия придать неверную окраску событию или сфальсифицировать факты.

Решение проблем

Борьба с информационной преступностью подобна борьбе с преступностью настоящей. Общее определение преступления описывает его как форму девиантного поведения человека, то есть поведения, отличного от обычного поведения человека, предписанного ему законами и нормами.

Организация интернета не предполагает наличия в себе какой-либо законодательной или исполнительной власти. С другой стороны, действия пользователя может регламентироваться законами стран, жителем которых является пользователь, или стран владельцев объектов, пострадавших от действий пользователей. Именно такая модель сейчас используется, но она сразу же породила, как защитную реакцию среды, «нейтральную» зону, расположенную в странах, где такие законы не действуют.

Вторым регулирующим фактором является запугивание. Несмотря на то, что случаи пойманных правонарушителей единичны, расследования и судебные процессы освещаются весьма широко, что вызывает у населения резонную мысль: «А ведь это мог быть я!». Страх заставляет пользователей быть более осторожными, и при отсутствии необходимости не скачивать лишней музыки, не устанавливать лишний раз программу.

Регулярно предпринимаются попытки тем или иным образом изменить саму структуру сети. Но отсутствие единого управляющего органа не дает возможность уничтожить текущий интернет и сделать новый, что, по мнению новых экспертов, могло бы решить большую часть современных проблем безопасности, в том числе информационной. Раз нет возможности изменить саму сеть, правительства разных стран предпринимают попытки сделать пользование сетью менее анонимной. По последнему заявлению, представитель МВД назвал сетевую анонимность приглашением к преступлению и призвал дать в этот "темный переулок" свет. Он добавил, что злоумышленники активно пользуются возможностью спрятаться под псевдонимом или укрыться на территории зарубежного государства и назвал защитников концепции свободного от регулирования интернета, оперирующих терминами "гласность" и "свобода слова" демагогами, потакающими преступникам.

Наиболее перспективной на сегодняшний день выглядит предложение, ограничить доступ в интернет до весьма узкого круга сайтов, предоставляя доступ к остальным ресурсам только при наличии некоего аналога «водительских прав», но для сети. Выдаваться эти права будут только при прохождении определенных курсов обучения с последующими экзаменами.

Не менее важным аспектом остается сетевой этикет. Большая часть интернет-ресурсов довольно жестоко подходят к пользователям, не соблюдающим общие нормы поведения, но все равно регулярно присутствуют люди, нецензурно выражающиеся, оскорбляющие участвующих в дискуссиях. При этом надо не забывать, что на определенном тематическом форуме могут пересечься совершенно представители разных возрастных групп, среди которых могут оказаться и школьники. И если взрослый человек, столкнувшись с грубостью и оскорблениями, может отреагировать, опираясь на свой богатый опыт, спокойно и сдержанно, то школьник может принять это за норму и начать общаться в той же манере.

Так же остается совершенно неразрешимая сторона проблемы информационной безопасности, связанная с действиями сотрудников разных стран, пытающихся узнать секретную информацию других стран, что по сути своей является шпионажем. Единственным возможным в настоящий момент решением является максимальное улучшение защиты информации для каждой страны, потому что альтернативой является полное изменение политических, социальных и культурных отношений между разными странами, когда все страны смогут вести между собой полностью открытую политику, или даже объединиться в некую единую сверхдержаву, что является недостижимым, утопическим вариантом.

Так же полностью моральную подоплеку имеет проблема кражи и фальсификации частной и корпоративной информации. Внимательность, использование защитных программ

и устройств, прохождение специализированного обучения, наем специалистов могут защитить информацию в большей части случаев, но корень проблемы остается в морали людей, пытающихся получить информацию — до тех пор, пока кто-то считает такое поведение приемлемым, будут необходимы специалисты по защите информации.

Выводы

В глубине веков люди впервые задумались о сохранности собственной переписки, сохранении собственных данных, и с тех пор формировалась дисциплина информационной безопасности. Методы передачи информации менялись, менялись методы ее защиты. Письма, книги, телеграф, радио, телевидение, компьютеры, локальные сети, интернет. Когда информации было мало, каждый способ был уникален и своеобразен, теперь, когда объемы информации стали огромны, появились методики защиты и рекомендации по безопасности. Угроз безопасности стало больше, так же появилось большое количество уязвимых мест, потребовалось изучение принципов и основ сохранения информации, разработка средств защиты, и как результат, появилась полноценная дисциплина, содержащая в себе многочисленные институты и немалый штат специалистов.

Как показывает внимательный анализ методов и причин угроз информационной безопасности людей, организаций и стран, основной причиной являются социальные и психологические факторы — чувство безнаказанности во время пребывания в сети, желание мести кому-либо, преступное любопытство. И, даже если организации и конечных пользователей можно защитить жестокими, тоталитарными методами контроля, то защитить государственную информацию от внимания представителей других стран можно лишь кардинально изменив самих людей, прекратив между ними чувство соперничества, сделав отношения между странами прозрачными и доверительными. Даже если объединить все страны в единую сверхдержаву, устроить тотальный контроль за всеми людьми, всегда найдутся недовольные, которые сформируют оппозицию, и война продолжится, в том числе информационная. Упразднение дисциплины информационной безопасности возможно будет лишь тогда, когда ни у кого не будет необходимости ничего скрывать.

Список использованных источников

1. Национальный стандарт РФ «Защита информации. Основные термины и определения» (ГОСТ Р 50922-2006).
2. Рекомендации по стандартизации «Информационные технологии. Основные термины и определения в области технической защиты информации» (Р 50.1.053-2005).
3. Лопатин В. Н. Информационная безопасность России: Человек, общество, государство Серия: Безопасность человека и общества. М.: 2000. — 428 с — ISBN 5-93598-030-4.
4. Стивен Леви ХАКЕРЫ, Герои Компьютерной Революции = Hackers, Heroes of the computer revolution. — «A Penguin Book Technology», 2002. — С. 337. — ISBN 0-14-100051-1
5. Скородумова О. Б. Хакеры // Знание. Понимание. Умение. — 2005. — № 4. — С. 159-161.
6. В.А.Каймин. Информатика. учебное пособие. 2-ое изд. М.РИОР,2007, 129с. ISBN 5-36900179-0
7. Щербаков А. Ю., Современная компьютерная безопасность. Теоретические основы. Практические аспекты. — М.:Книжный мир, 2009. — 352 с — ISBN 978-5-8041-0378-2.
8. Лепехин А. Н. Расследование преступлений против информационной безопасности. Теоретико-правовые и прикладные аспекты. М.: Тесей, 2008. — 176 с — ISBN 978-985-463-258-2.
9. Бармен Скотт. Разработка правил информационной безопасности. М.: Вильямс, 2002. — 208 с — ISBN 5-8459-0323-8, ISBN 1-5787-0264-X.