Содержание:

ВВЕДЕНИЕ

На сегодняшний момент тяжело представить современный мир без тех технологий, которыми люди пользуются. Каждая компания и организация использует различные технические устройства, многие процессы автоматизированы, множество систем работает по написанным программам, а человеку остаётся лишь контролировать процесс исполнения деятельности, и писать новые программы для большего ускорения процессов. С помощью современных программ, а также компьютерных технологий, люди достигли больших высот и преобразований почти во всех сферах жизни общества.

Однако, это имеет свои уязвимые аспекты, во-первых, человек стал зависим от своих технологий, во- вторых, теперь уязвимость одной технологии может привести к полной уязвимости организации, и есть те, кто может этим воспользоваться в корыстных целях.

Несомненно, обычный пользователь персонального компьютера в большинстве случаев не может обезопасить даже свой компьютер, именно поэтому появилась такая специальность как информационная безопасность, её главная цель – это обеспечение безопасности информации.

Объект исследования – информация.

Предмет исследования – различные виды угроз информационной безопасности.

Целью работы является исследование изучение информационной безопасности и ее видов угроз.

Достижение поставленной цели предполагает решение следующих задач:

1. Изучить понятие информационной безопасности: цели, задачи, принципы.

2. Охарактеризовать основные угрозы информационной безопасности.

3. Определить проблемы и меры защиты информационной безопасности.

4. Охарактеризовать основные методы, средства и правила защиты информации.

ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ УГРОЗ БЕЗОПАСНОСТИ РАБОТЫ В СЕТИ ИНТЕРНЕТ

1.1 Понятие информационной безопасности: цели, задачи, принципы

С развитием средств информационных коммуникаций, а, следовательно, и возможности нанесения ущерба информации, которая хранится и передается с их помощью, возникла информационная безопасность (ИБ).

Информационная безопасность (англ. «Information security») – защищенность информации и соответствующей инфраструктуры от случайных или преднамеренных воздействий, сопровождающихся нанесением ущерба владельцам или пользователям информации[1].

Цель защиты информации – минимизация потерь, вызванных нарушением целостности или конфиденциальности данных, а также их недоступности для потребителей.

Концептуальная модель безопасности информации представлена на рис. 1.1.

Рисунок 1.1 Концептуальная модель безопасности информации

Основными целями обеспечения информационной безопасности является защита государственной тайны, конфиденциальной информации общественного значения и личности, защита от информационного воздействия[2].

Основной задачей обеспечения ИБ является реализация многоплановых и комплексных мер по устранению и отслеживанию несанкционированного доступа неавторизованных лиц, а также действий, которые предупреждают о неправомерном использовании, повреждении, искажении, копированием, блокировании информации.

Основные принципы информационной безопасности[3]:

1. Целостность данных является свойством, в соответствии с которым информация сохраняет свое содержание и структуру в процессе ее передачи и хранения. Только пользователь с правом доступа может создавать, уничтожать или изменять данные.

2. Конфиденциальность — свойство, которое указывает на необходимость ограничения доступа к конкретной информации для обозначенного круга лиц. Таким образом, конфиденциальность дает гарантию того, что в процессе передачи данных, они могут быть известны только авторизованным пользователям.

3. Доступность информации — это свойство характеризует способность обеспечивать своевременный и беспрепятственный доступ полноправных пользователей к требуемой информации.

4. Достоверность – данный принцип выражается в строгой принадлежности информации субъекту, который является ее источником или от которого она принята.

Вопросы информационной безопасности становятся первоочередными в тех случаях, когда выход из строя или возникновение ошибки в конкретной компьютерной системе могут привести к тяжелым последствиям.

Информационная безопасность определяется способностью ее субъекта (государства, общества, личности)[4]:

- обеспечивать информационные ресурсы для поддержания своего устойчивого функционирования и развития;

- противостоять информационным угрозам, негативным воздействиям на сознание и психику людей, а также на компьютерные сети и другие технические источники информации;

- вырабатывать навыки и умения безопасного поведения;

- поддерживать постоянную готовность к адекватным мерам защиты информации.

Защита информации осуществляется проведением комплекса мероприятий, направленных на обеспечение ИБ.

Для решения проблем информационной безопасности нужно прежде всего выявить субъекты информационных отношений и их интересы, связанные с использованием информационных систем (ИС). Оборотной стороной использования информационных технологий являются угрозы ИБ.

Нарушения доступности, целостности и конфиденциальности информации могут быть вызваны различными опасными воздействиями на информационные компьютерные системы.

Таким образом, подход к обеспечению ИБ может существенно различаться для разных категорий субъектов. Для одних на первом месте стоит секретность информации (например, государственные учреждения, банки, военные институты), для других эта секретность практически не важна (например, образовательные структуры).

Кроме того, ИБ не сводится только к защите от несанкционированного доступа к информации. Субъект информационных отношений может пострадать (понести убытки или получить моральный ущерб), например, от поломки системы, которая вызовет перерыв в работе ИС. Примером такого проявления могут быть те же образовательные структуры, для которых сама защита от несанкционированного доступа к информации не так важна, как важна работоспособность всей системы.

Самым слабым звеном в обеспечении информационной безопасности чаще всего оказывается человек.

1.2 Обзор угроз информационной безопасности

Угроза – это потенциально возможное событие, действие, которое посредством воздействия на объект защиты может привести к нанесению ущерба[5].

Угроза информационной безопасности – совокупность условий и факторов, которые создают опасность нарушения информационной безопасности.

Попытка реализации угрозы называется атакой, а предпринимающий такую попытку – злоумышленником.

Источники угроз представлены людьми, техническими устройствами, моделями, алгоритмами, программами, технологическими схемами обработки, внешней средой.

Основными причинами появления угроз информационной безопасности являются:

- объективные причины, которые не связаны напрямую с деятельностью человека и вызывают случайные угрозы;

- субъективные причины, которые связаны с деятельностью человека и вызывают умышленные (деятельность иностранных разведок, уголовных элементов и др.) и случайные (плохое психофизиологическое состояние, плохая подготовка и др.) угрозы информации.

Стоит заметить, что отдельные угрозы нельзя считать следствием какой-то ошибки. Например, существует угроза сбоя в подаче электричества, которая зависит от необходимости аппаратного обеспечения ИС в электропитании.

Сегодня выделяют огромное количество угроз информационной безопасности, которые классифицирует по разным критериям.

Рассмотрим основные виды угроз информационной безопасности.

По природе возникновения выделяют:

- искусственные угрозы безопасности, вызванные деятельностью человека;

- природные (естественные) угрозы, созданные воздействиями на информационную систему объективных физических действий или стихийных природных явлений.

По степени зависимости от активности угрозы ИБ разделяют на:

- угрозы – только в ходе обработки данных, к примеру угрозы реализации и рассылке программных вирусов;

- независимо от активности, к примеру вскрытие шифров (поточные шифры или блочное шифрование или shema_Rabina) криптозащиты информации.

По аспекту ИБ (доступность, целостность, конфиденциальность), против которого направлены угрозы.

Угрозы доступности – ограничение или блокирование доступа к данным (например, невозможность подключится к серверу с базой данных в результате DDoS-атаки).

Наиболее распространенными угрозами доступности и опасными с точки зрения материального ущерба являются случайные ошибки рабочего персонала, использующего информационные системы[6].

К таким ошибкам можно отнести неправильно введенные данные, которые могут привести к необратимым последствиям.

Также подобные ошибки могут создать уязвимое место, которым могут воспользоваться злоумышленники. Такие ошибки могут допускаться, к примеру, администраторами ИС. Считают, что до 65% потерь составляют последствия именно случайных ошибок[7]. Это доказывает, что безграмотность и небрежность в работе приносят гораздо больше вреда, чем другие факторы.

К угрозам доступности также относится отказ пользователей из-за нежелания работать с ИС, невозможности работать с ИС (недостаточная подготовка, низкая компьютерная грамотность, отсутствие технической поддержки и т.п.).

Внутренний отказ ИС рассматривают как угрозу доступности, источниками которого может быть:

- случайное или умышленное отступление от правил эксплуатации;

- выход системы из штатного режима эксплуатации в силу случайных или умышленных действий пользователей или персонала (превышение дозволенного числа запросов, превышение объема информации, которая обрабатывается, и т.п.);

- ошибки в конфигурировании системы;

- отказ программного или аппаратного обеспечения;

- поломка или повреждение аппаратуры; повреждение данных.

Угрозы целостности – несанкционированная модификация, дополнение или уничтожение данных (например, внесение изменений в бухгалтерские проводки с целью хищения денежных средств).

Так же стоит разделять на угрозы целостности служебной информации и содержательных данных. Под служебной информацией понимаются пароли для доступа, маршруты передачи данных в локальной сети и подобная информация. Чаще всего и практически во всех случаях злоумышленником осознанно или нет, оказывается сотрудник организации, который знаком с режимом работы и мерами защиты[8].

С целью нарушения статической целостности злоумышленник может: ввести неверные данные, изменить данные.

Угрозы динамической целостности представлены переупорядочением, кражей, дублированием данных или внесением дополнительных сообщений.

Угрозы конфиденциальности – несанкционированный доступ к данным (например, получение посторонними лицами сведений о состоянии счетов клиентов банка).

Конфиденциальную информацию делят на предметную и служебную. Служебная информация (например, пароли пользователей) не принадлежит к конкретной предметной области, она выполняет техническую роль, но ее раскрытие особенно опасно, т.к. это приведет к получению несанкционированного доступа ко всей информации, в том числе предметной[9].

Также выделяют угрозы по степени преднамеренности проявления - случайные и преднамеренные.

Случайные, или непреднамеренные угрозы представляют собой угрозы, не связанные с действиями злоумышленников.

Источником случайных реакций могут быть[10]:

- отрешение и сбои аппаратурных устройств;

- упущении в работе обслуживающих сотрудников и других служащих;

- критичные ситуации из-за стихийных несчастий и отключений электрического питания;

- шумы и фон в каналах связи из-за влияния внешних факторов (характеристики проводных линий связи при передаче данных и внутренний фактор — полоса пропускания и пропускная способность) канала;

- погрешности в программном обеспечении (ПО);

- спецификация физической среды Ethernet или token ring.

Погрешности в ПО случаются распространенным видом компьютерных повреждений. ПО рабочих станций, серверов, маршрутизаторов и т д. разработано людьми, поэтому оно может содержать ошибки. Если сложность подобного ПО выше, то и больше риск раскрытие в нем ошибок и уязвимых узлов. Некоторые из них могут не представляют никакой угрозы, а некоторые же могут привести к вещественным результатам, таким как неработоспособность серверной платформы, получение похитителем контроля над серверной платформой, несанкционированное эксплуатация ресурсов (использование ПК в качестве площадки для дальнейших атак и т.п.). Принцип похожие погрешности устраняются с помощью паков обновлений, которые регулярно выпускают разработчики ПО. На сегодня своевременное обновление таких паков является необходимым пунктом безопасности информации. Также погрешности в сети могу случатся из-за проблем защиты информации в сети[11].

Преднамеренные угрозы связаны с целенаправленными действиями нарушителя. Изучение этого класса затруднено, так как он имеет очень динамичный характер и постоянно пополняется новыми видами угроз.

По рангу преднамеренности выражения:

- угрозы, спровоцированы ошибками или небрежностью сотрудников, например неграмотное использование методов защиты, ввод неверных данных и т.п.;

- угрозы преднамеренного влияния, например методы мошенников.

Разделяют угрозы в зависимости от их непосредственного источника:

- природной среды (стихийные бедствия);

- человека (разглашение конфиденциальных данных);

- программно-аппаратных средств: санкционированные (ошибка в работе операционной системы) и несанкционированные (заражение системы вирусами).

Несанкционированный доступ (НСД) — самый распространенный и многовариативный вид компьютерных правопреступлений. Концепция НСД заключается в получении личности (нарушителем) доступа к объекту в попирании свода правил разграничения доступа, созданных в соответствии с принятой политикой безопасности. НСД использует погрешность в системе защиты и возможен при неправильном выборе методов защиты, их некорректной настройке и установке. НСД осуществляется как локальными методами, так и специально сотворенными программными и аппаратными методами[12].

Основные пути НСД, через которые преступник может сформировать доступ к элементам и осуществить утягивание, изменение и/или удаление данных[13]:

- технологические панели регулирования;

- косвенные электромагнитные излучения от каналов связи, аппаратуры, сетей заземления и электропитания и др.;

- каналы связи между аппаратными компонентами;

- локальные линии доступа к данным (терминалы сотрудников, администратора системы, оператора);

- межсетевой экран;

- методы отображения и записывание данных или методы обнаружения ошибок.

- через seti_PDH и seti_dwdm.

Самые распространенные нарушения НСД – это перехват паролей (производится с помощью специально разработанных программ), выполнение каких-либо действий под именем другого человека, а также использование злоумышленником привилегий законных пользователей.

Источник угроз может иметь разное положение. В зависимости от этого фактора также выделяют три группы[14]:

- непосредственно в самой системе, к примеру неточная реализация ресурсов системы;

- в пределах зоны информационной системы, к примеру использование подслушивающих приборов, записей, хищение распечаток, носителей данных и т.п.;

- вне зоны информационной системы, например захват информации, передаваемых по путям связи, захват побочных акустических, электромагнитных и других излучений устройств.

Угрозы могут оказывать различное воздействие на компьютерную систему. По данному признаку выделяют угрозы:

- с пассивными воздействиями, реализация которых не влечет за собой изменение структуры данных (например, копирование);

- угрозы с активными воздействиями — это такие, которые, наоборот, меняют структуру и содержание компьютерной системы (внедрение специальных программ).

Выделяют угрозы по месту расположения в системе: угрозы доступа к информации, находящейся на внешних запоминающих устройствах, в оперативной памяти и к той, что циркулирует в линиях связи.

По способу пути к ресурсам[15]:

- угрозы, реализуемые с использованием маскированного нестандартного каналу пути к ресурсам, к примеру несанкционированный путь к ресурсам путем использования каких-либо возможностей ОС;

- угрозы, реализуемые с использованием стандартного каналу доступа к ресурсам, к примеру незаконное обретение паролей и других параметров разграничения доступа с последующей маскировкой под зарегистрированного сотрудника.

По шагам доступа сотрудников или программ к ресурсам[16]:

- угрозы, реализуемые после согласия доступа к ресурсам, к примеру угрозы некорректного или несанкционированного применение ресурсов;

- угрозы, реализуемые на шаге доступа к ресурсам, к примеру угрозы несанкционированного доступа.

Угрозы могут использовать прямой стандартный путь к ресурсам с помощью незаконно полученных паролей или посредством неправомерного применения терминалов законных пользователей, а могут «обойти» существующие средства защиты иным путем.

Такие действия, как хищение информации, относят к угрозам, проявляющимся независимо от активности системы.

Также можно выделить технические угрозы информационной безопасности – вредоносные программы, ботнеты и DoS и DDoS-атаки.

Ошибки в программном обеспечении – это самое узкое место любой сети. Программное обеспечение серверов, рабочих станций, маршрутизаторов и т. д. написано людьми, следовательно, оно практически всегда содержит ошибки. Чем выше сложность подобного ПО, тем больше вероятность обнаружения в нем ошибок и уязвимостей[17]. Большинство из них не представляет никакой опасности, некоторые же могут привести к трагическим последствиям, таким, как получение злоумышленником контроля над сервером, неработоспособность сервера, несанкционированное использование ресурсов. Большинство таких уязвимостей устраняется с помощью пакетов обновлений, регулярно выпускаемых производителем программного обеспечения. Своевременная установка таких обновлений является необходимым условием безопасности сети.

DoS-атака (отказ в обслуживании) – это атака, приводящая к парализации работы сервера или персонального компьютера вследствие огромного количества запросов, с высокой скоростью поступающих на атакуемый ресурс[18].

Суть DoS-атаки заключается в том, что злоумышленник пытается сделать временно недоступным конкретный сервер, перегрузить сеть, процессор или переполнить диск. Цель атаки – просто вывести компьютер из строя, а не получить информацию, захватить все ресурсы компьютера-жертвы, чтобы другие пользователи не имели к ним доступа. К ресурсам относятся: память, процессорное время, дисковое пространство, сетевые ресурсы и т. д.

Осуществить DoS-атаку можно двумя способами[19]:

1. При первом способе для DoS-атаки используется уязвимость программного обеспечения, установленного на атакуемом компьютере. Уязвимость позволяет вызвать определенную критическую ошибку, которая приведет к нарушению работоспособности системы.

2. При втором способе атака осуществляется при помощи одновременной отсылки большого количества пакетов информации на атакуемый компьютер, что вызывает перегрузку сети.

Если подобная атака проводится одновременно сразу с большого числа компьютеров, то в этом случае говорят о DDoS-атаке.

DDoS-атака (распределенный отказ в обслуживании) – это разновидность DoS-атаки, которая организуется при помощи очень большого числа компьютеров, благодаря чему атаке могут быть подвержены сервера даже с очень большой пропускной способностью Интернет-каналов[20].

Для организации DDoS-атак злоумышленники используют ботнет – специальную сеть компьютеров, зараженных особым видом вирусов. Каждым таким компьютером злоумышленник может управлять удаленно, без ведома владельца. При помощи вируса или программы, искусно маскирующейся под легальную, на компьютер-жертву устанавливается вредоносный программный код, который не распознается антивирусом и работает в фоновом режиме. В нужный момент по команде владельца ботнета такая программа активизируется и начинает отправлять запросы на атакуемый сервер, в результате чего заполняется канал связи между сервисом, на который проводится атака, и Интернет-провайдером и сервер перестает работать.

Новый тип атак DDoS отличается от предыдущего наличием огромного количества компьютеров, расположенных в большой географической зоне. Такие атаки просто перегружают канал трафиком и мешают прохождению, а зачастую и полностью блокируют передачу по нему полезной информации. Особенно актуально это для компаний, занимающихся каким-либо online-бизнесом, например, торговлей через Internet.

Вирусы — старая категория опасностей, которая в последнее время в чистом виде практически не встречается. В связи с активным применением сетевых технологий для передачи данных вирусы все более тесно интегрируются с троянскими компонентами и сетевыми червями. В настоящее время компьютерный вирус использует для своего распространения либо электронную почту, либо уязвимости в ПО. А часто и то, и другое. Теперь на первое место вместо деструктивных функций вышли функции удаленного управления, похищения информации и использования зараженной системы в качестве плацдарма для дальнейшего распространения. Все чаще зараженная машина становится активным участником DDoS-атак[21]. Методов борьбы достаточно много, одним из них является все та же своевременная установка обновлений.

В анализаторы протоколов и «снифферы» включают средства перехвата передаваемых по сети данных. Такие средства могут быть как аппаратными, так и программными. Обычно данные передаются по сети в открытом виде, что позволяет злоумышленнику внутри локальной сети перехватить их. Некоторые протоколы работы с сетью (POPS, FTP) не используют шифрование паролей, что позволяет злоумышленнику перехватить их и использовать самому. При передаче данных по глобальным сетям эта проблема встает наиболее остро. По возможности следует ограничить доступ к сети неавторизированным пользователям и случайным людям.

К техническим средствам съема информации относят такие средства, как клавиатурные жучки, различные мини-камеры, звукозаписывающие устройства и т.д. Данная группа используется в повседневной жизни намного реже вышеперечисленных, так как, кроме наличия спецтехники, требует доступа к сети и ее составляющим[22].

Большинство злоумышленников полагается не только на технологии, но и на человеческие слабости, используя при этом социальную инженерию. Этот сложный термин обозначает способ получать нужную информацию не с помощью технических возможностей, а путем обыкновенного обмана, хитрости. Социальные инженеры применяют психологические методы воздействия на людей через электронную почту, социальные сети и службы мгновенного обмена сообщениями. В результате их умелой работы пользователи добровольно выдают свои данные, не всегда понимая, что их обманули.

Мошеннические сообщения чаще всего содержат угрозы, например, закрытия пользовательских банковских счетов, обещания огромного выигрыша с минимальными усилиями или вовсе без них, запросы о добровольных пожертвованиях от лица благотворительных организаций. Чаще всего злоумышленники не оставляют пользователю времени для размышлений, например, просят заплатить в день получения письма.

Еще одной, получившей распространение в последнее время, угрозой является шантаж пользователя при помощи вредоносного скрипта. Загружая инфицированную страницу или скачивая информацию из сети, пользователь невольно устанавливает на свой компьютер вредоносный скрипт. Такой скрипт, как правило, инициирует открытие окна, закрывающей весь рабочий стол или окно браузера. Надпись обычно содержит дискриминирующую пользователя информацию или картинку. При этом не скрывается, что для закрытия окна

требуется отправить смс на предложенный номер. Обычно указывается стоимость в 5-10 рублей. На самом деле с баланса снимается большая сумма или весь баланс. Иногда такой смс вирус вымогает с пользователя до нескольких тысяч рублей. При этом нет никакой гарантии того, что окно после этого будет закрыто[23].

Фишинг – это всё более популярный тип интернет-мошенничества, с помощью которого пытаются получить конфиденциальные данные от пользователей, чтобы затем использовать, например, для получения контроля над банковским счетом[24].

Цель фишинга – получение доступа к конфиденциальным данным, таким как адрес, телефон, номера кредитных карт, логины и пароли, путем использования поддельных веб-страниц.

Попытки вытянуть ключевую информацию очень часто принимают форму поддельных писем – от почты России, банка или другой организации, которой большинство пользователей доверяет. С угрозами этого типа имели в своей жизни дело почти 60% пользователей (по данным исследования Intel до 15% российских интернет-пользователей).

Фарминг – это, в свою очередь, более развитая и часто труднее различимая форма фишинга, использующая подлинные адреса учреждений, но перенаправляющая на поддельные копии страниц[25].

Таким образом, список опасностей гораздо больше и постоянно расширяется. Каждая из них представляет собой, однако, действительно серьезную угрозу, которая из-за невнимательности пользователя может привести к ситуации, в которой он теряет доступ к критически важным данным. Самой большой угрозой, как показывает практика, является человек. Неосторожность пользователей часто становится причиной поломки компьютеров.

ГЛАВА 2. МЕРЫ, МЕТОДЫ И СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИИ НА СОВРЕМЕННОМ ЭТАПЕ

2.1 Проблемы и меры защиты информационной безопасности

Формирование режима информационной безопасности – это проблема комплексная.

Меры по ее решению можно подразделить на пять уровней[26]:

- законодательный (законы, нормативные акты, стандарты и т.п.);

- морально-этический (всевозможные нормы поведения, несоблюдение которых ведет к падению престижа конкретного человека или целой организации);

- административный (действия общего характера, предпринимаемые руководством организации);

- физический (механические, электро- и электронно-механические препятствия на возможных путях проникновения потенциальных нарушителей);

- аппаратно-программный (электронные устройства и специальные программы защиты информации).

Выделим основные функции организационно-правовой базы[27]:

1. Разрабатывать основные принципы отнесения сведений, которые имеют конфиденциальный характер, к защищаемой информации.

2. Определить системы органов и должностных лиц, которые отвечают за обеспечение информационной безопасности в стране, и порядок регулирования деятельности предприятия и организации в этой области.

3. Создать полный комплекс нормативно-правовых руководящих и методических документов, которые регламентируют вопросы обеспечения информационной безопасности страны в целом и конкретного объекта.

4. Определить меры ответственности за нарушение правил защиты.

5. Определить порядок решения спорных и конфликтных ситуаций, связанных с вопросами защиты информации.

Юридическую основу организационно-правового обеспечения защиты информации составляют законы и другие нормативно-правовые акты для достижения следующих целей:

- правила по защите информации являются обязательными для соблюдения всеми лицами, которые имеют отношение к конфиденциальной информации;

- узаконивание всех мер ответственности за нарушение правил защиты информации;

- узаконивание (приобретение юридической силы) технико-математических решений вопросов организационно-правового обеспечения защиты информации;

- узаконивание процессуальных процедур разрешения ситуаций, которые складываются в процессе функционирования системы защиты.

Единая совокупность всех этих мер, направленных на противодействие угрозам безопасности с целью сведения к минимуму возможности ущерба, образуют систему защиты.

Надежная система защиты должна соответствовать следующим принципам[28]:

1. Стоимость средств защиты должна быть меньше, чем размеры возможного ущерба.

2. Каждый пользователь должен иметь минимальный набор привилегий, необходимый для работы.

3. Защита тем более эффективна, чем проще пользователю с ней работать.

4. Возможность отключения в экстренных случаях.

5. Специалисты, имеющие отношение к системе защиты, должны полностью представлять себе принципы ее функционирования и в случае возникновения затруднительных ситуаций адекватно на них реагировать.

6. Под защитой должна находиться вся система обработки информации.

7. Разработчики системы защиты, не должны быть в числе тех, кого эта система будет контролировать.

8. Система защиты должна предоставлять доказательства корректности своей работы.

9. Лица, занимающиеся обеспечением информационной безопасности, должны нести личную ответственность.

10. Объекты защиты целесообразно разделять на группы так, чтобы нарушение защиты в одной из групп не влияло на безопасность других.

11. Надежная система защиты должна быть полностью протестирована и согласована.

12. Защита становится более эффективной и гибкой, если она допускает изменение своих параметров со стороны администратора.

13. Система защиты должна разрабатываться, исходя из предположения, что пользователи будут совершать серьезные ошибки и, вообще, имеют наихудшие намерения.

14. Наиболее важные и критические решения должны приниматься человеком.

15. Существование механизмов защиты должно быть по возможности скрыто от пользователей, работа которых находится под контролем.

Необходимость обеспечения безопасности данных связана со следующими причинами[29]:

1. Непосредственными расходами на восстановление и простой.

2. Снижением доверия клиентов.

3. Опасностью судебного преследования.

4. Собственно потерей и/или разглашением секретных данных. Не поддается оценке, ущерб просто может быть огромен, вплоть до банкротства фирмы.

Инвестиции организаций в обеспечение информационной безопасности в виде приобретаемых средств защиты, затрат на оплату труда специалистов, на проведение внешнего аудита безопасности и т. п., неуклонно увеличиваясь из года в год, зачастую не окупаются. Происходит это по причине того, что большинство организаций продолжают придерживаться фрагментарного подхода, который оправдывает себя только при слабой зависимости организации от ИТ и низком уровне рисков информационной безопасности. Адекватный уровень информационной безопасности в состоянии обеспечить только комплексный подход, предполагающий планомерное использование как программно-технических, так и организационных мер защиты на единой концептуальной основе. При этом организационные меры играют первостепенную роль. Но если

пользователи игнорируют элементарные правила парольной политики, а сетевые администраторы нарушают установленные процедуры предоставления доступа к ресурсам корпоративной сети, то эффективность механизмов защиты сводится к нулю.

2.2 Методы, средства и правила защиты информации

Сетевая безопасность представляет собой комплекс мер, основной задачей которых является предотвращение кражи конфиденциальных данных и любое другое нарушение нормальной работы компьютера вследствие несанкционированного доступа к нему извне.

Методы обеспечения безопасности информации[30]:

1. Препятствие - физическое преграждение пути злоумышленнику к защищаемой информации (например, коммерчески важная информация хранится на сервере внутри здания компании, доступ в которое имеют только ее сотрудники).

2. Управление доступом – регулирование использования информации и доступа к ней за счет системы идентификации пользователей, их опознавания, проверки полномочий и т.д. (например, когда доступ в отдел или на этаж с компьютерами, на которых хранится секретная информация, возможен только по специальной карточке-пропуску. Или когда каждому сотруднику выдается персональный логин и пароль для доступа к базе данных предприятия с разными уровнями привилегий).

3. Криптография – шифрование информации с помощью специальных алгоритмов (например, шифрование данных при их пересылке по Интернету; или использование электронной цифровой подписи).

4. Противодействие атакам вредоносных программ (англ. «malware») – предполагает использование внешних накопителей информации только от проверенных источников, антивирусных программ, брандмауэров, регулярное выполнение резервного копирования важных данных и т.д. (вредоносных программ очень много, и они делятся на ряд классов: вирусы, эксплойты, логические бомбы, трояны, сетевые черви и т.п.).

5. Регламентация – создание условий по обработке, передаче и хранению информации, в наибольшей степени обеспечивающих ее защиту (специальные нормы и стандарты для персонала по работе с информацией, например, предписывающие в определенные числа делать резервную копию электронной документации, запрещающие использование собственных флеш-накопителей и т.д.).

6. Принуждение – установление правил по работе с информацией, нарушение которых карается материальной, административной или даже уголовной ответственностью (штрафы, закон «О коммерческой тайне» и т.п.).

7. Побуждение – призыв к персоналу не нарушать установленные порядки по работе с информацией, т.к. это противоречит сложившимся моральным и этическим нормам (например, Кодекс профессионального поведения членов «Ассоциации пользователей ЭВМ США»).

Далее рассмотрим средства защиты информации[31]:

1. Технические (аппаратные) средства – сигнализация, решетки на окнах, генераторы помех воспрепятствования передаче данных по радиоканалам, электронные ключи и т.д.

2. Программные средства – программы-шифровальщики данных, антивирусы, системы аутентификации пользователей и т.п.

3. Смешанные средства – комбинация аппаратных и программных средств.

4. Организационные средства – правила работы, регламенты, законодательные акты в сфере защиты информации, подготовка помещений с компьютерной техникой и прокладка сетевых кабелей с учетом требований по ограничению доступа к информации и пр.

Также рассмотрим некоторые правила защиты от кражи личных данных.

Для защиты от кражи личных данных и сетевого мошенничества необходимо[32]:

- Использовать на компьютере надежное программное обеспечение для безопасности работы в сети интернет. Это поможет защитить его от вирусов, шпионских программ, спама и другого вредоносного программного обеспечения, предназначенного для кражи личной информации.

- Находясь в Интернете, нужно быть осмотрительным. Если необходимо ввести личную информацию, то нужно указывать только самое необходимое. Использовать пароли, которые трудно угадать, и менять их регулярно.

- Не загружать файлы из Интернета, если не уверены в их безопасности. Вместе с полезными приложениями иногда могут загружаться вредоносные программы. Чтобы иметь уверенность в том, что сайты, с которых выполняется загрузка, являются надежными, а загружаемые файлы — безопасными, регулярно обновлять программное обеспечение. Быть особенно осторожным при загрузке исполняемых файлов (названия которых заканчиваются на «.exe»)[33].

- Совершать покупки в Интернете осторожно. Нужно ознакомиться с политиками сайта в отношении конфиденциальности и безопасности, в которых оговаривается, какая информация собирается, как обеспечивается ее защита и кому она предоставляется. Для оплаты покупок использовать кредитную карту — так проще всего защититься от мошенничества. Регулярно проверять выписку по кредитной карте, чтобы убедиться в том, что никто не пользовался, и незамедлительно сообщать обо всех случаях мошенничества в компанию.

- Не хранить свои пароли на компьютере, в том числе ключи от платежных систем. При запросе браузера о сохранении паролей, всегда отвечайте «не сейчас» или внесите соответствующие настройки. Не сохраняйте логины и пароли в текстовых документах на компьютере. Некоторые «трояны» их находят и там. Тем более не хранить их в интернете на электронной почте[34].

- Не посещать сайты сомнительного содержания. Конечно, иногда пользователь заходит на них случайно. Если это случилось, как можно быстрее нужно закрыть сайт, пока он не успел полностью загрузиться. Особенно много сайтов, которые заражены вирусами или устанавливают вредоносные скрипты в порнографических видео и аудио тематиках.

- Делайте резервные копии всех своих данных. Можно записать все важные файлы на оптический диск или на внешний жесткий диск. Можно на флеш-карту, но стоит помнить, что современные карты не живут десятилетиями, поэтому карту раз в 3 года нужно менять. Или же можно воспользоваться облачным хранилищем. Этот способ самый оптимальный. Сейчас многие компании предоставляют бесплатные услуги облачного хранилища. Например, Google Drive, DropBox, Hive.im, Mega и пр. Бесплатно предоставляется обычно небольшое хранилище 5-10 Гб, но бывают и исключения, например сервис mega.co.nz предоставляет бесплатно целых 50

гигабайт. Если информация очень важная желательно разместить ее не в одном, а в нескольких облачных хранилищах и даже при физическом уничтожении компьютера можно получить свои данные назад.

В настоящее время актуально применение правил безопасности в социальных сетях[35]:

- Соблюдать конфиденциальность. Необходимо ознакомиться параметрами конфиденциальности на сайтах социальных сетей и изучить их правила в отношении конфиденциальности и безопасности данных.

- Защитить компьютер. Использовать надежное программное обеспечение для защиты компьютера и регулярно обновлять его.

- Заходить на свою почту, страницы в социальных сетях только с сервиса, от которого она предоставлена, т.к. для кражи паролей злоумышленники достаточно часто используют обычный обман, полагаясь на невнимательность пользователя и не желание читать и вникать в прочитанное.

- Уяснить для себя, какой информацией можно делиться.

- Уважать авторские права и избегать несанкционированного использования или распространения материалов, охраняемых авторским правом, в своих профилях.

- Сообщать о проблемах. Ставить администрацию сайта в известность о нежелательных контактах и неприемлемом содержимом.

Таким образом, чтобы минимизировать риск взлома информационной сети нужно [36]:

1. В первую очередь необходимо обеспечить физическую безопасность. Доступы во все серверные и коммутационные комнаты должен быть предоставлен ограниченному числу сотрудников. Если используются точки доступа, они должны быть максимально скрыты что бы избежать к ним физический доступ. Данные должны иметь физические резервные копии. Утилизация жёстких дисков должна проходить под строгим контролем. Ведь получив доступ к данным, последствия могут быть печальными.

2. Позаботится о внешней безопасности. Первый «защитник сети», выступает farewall или межсетевой экран, обеспечивающий защиту от несанкционированного удалённого доступа.

Сеть можно разделить на подсети для ограничения серверов от пользователей. Использование фильтрующего маршрутизатора, который фильтрует исходящие и входящие потоки. Все устройства подключение к сети буду иметь доступ в интернет, а обратно доступ к устройствам из Интернета блокируется.

3. Разграничения в ролях администраторов и пользователей:

- доступ к серверам не должен иметь рядовой пользователь;

- доступ управления конфигурацией компьютеров должен иметь только администратор;

- доступ к сетевым ресурсам должны иметь каждый там, где ему это необходимо для выполнения должностных обязанностей;

- трафик всех сотрудников должен фильтроваться, и в этом поможет прокси-сервер;

- каждый пользователь должен устанавливать сложный пароль, и не должен не кому его передавать. Даже IT специалисты его не знают.

4. Антивирусная защита является главным рубежом защиты корпоративной сети от внешних атак. Комплексная антивирусная защита минимизирует проникновения в сеть вирусов. В первую очередь необходимо защитить сервера, рабочие станции, шлюзы и систему корпоративной почты

5. Установка актуальных обновлений программного обеспечения.

6. Защита сети через виртуальные частные сети VPN. В связи со спецификой работы организаций, как показывает практика, многие сотрудники осуществляют рабочую деятельность удалённо, в связи с этим необходимо обеспечить максимальную защиту трафика, а реализовать это помогут шифрованные туннели VPN.

7. Безопасность корпоративной почты. Компании, которые обрабатывают большое количество электронной почты, в первую очередь подвержены фишинг атакам. Чтобы решить данную проблему рекомендуется использовать следующие методы [37]:

- использование спам списков (рейтинг почтовых сервисов);

- анализ вложения письма (должен осуществляться анализ не только текста, но и самих вложений);

- определение массовости письма (большинство почтовых серверов имеют такую функцию, можно посмотреть, кому в почтовые ящики упали письма).

8. Никакая система не защитит от человеческого фактора. Все сотрудники компании, вне зависимости от должности должны понимать и главное соблюдать правила информационной безопасности. Любые посторонние файлы, скаченные из сети или из почты, могут быть опасны и нести в себе угрозу, а также внешние накопители информации, которые не относятся к рабочему процессу.

Договориться, чтобы перед информированием сотрудника об увольнении, сначала сообщили вам, а вы продумали ряд мероприятий, для защиты рабочих документов данного сотрудника от кражи или порчи.

А также повышать квалификацию работников в области информационной безопасности и компьютерной грамотности.

Пользуясь вышеприведенными методами, средствами и правилами информационно безопасности, можно существенно уменьшить риск получить вирус на свой компьютер или потерять учетную запись на любимом сайте.

Таким образом, безопасность в современном информационном мире зависит от предусмотрительности и осведомленности каждого гражданина. Если использовать на практике вышеуказанные рекомендации, то работа в интернет станет намного безопаснее, и пользователи не будут бояться потерять свои личные данные и деньги.

ЗАКЛЮЧЕНИЕ

Под понятием «информационная безопасность» часто понимают защищенность информации и поддерживающей инфраструктуры (системы электро-, водо- и теплоснабжения, кондиционеры, средства коммуникаций и обслуживающий персонал) от любых воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений.

Угроза информационной безопасности – совокупность условий и факторов, которые создают опасность нарушения информационной безопасности.

Существует два основных вида угроз, которым могут подвергаться пользователи: технические (вредоносные программы, ботнеты и DoS и DDoS-атаки) и социальная инженерия (фишинг и фарминг).

Виду угроз информационной безопасности:

1. По природе возникновения: естественные и искусственные.

2. По степени преднамеренности проявления: случайные и преднамеренные.

3. В зависимости от их непосредственного источника: санкционированные и несанкционированные.

4. По положению источника угроз: угрозы, источник которых находятся вне контролируемой группы компьютерной системы; угрозы, источник которых – в пределах контролируемой зоны системы; угрозы, находящиеся непосредственно в самой системе

5. По различному воздействию на компьютерную систему: угрозы с пассивными воздействиями; угрозы с активными воздействиями.

6. По этапам доступа пользователей или программ к ресурсам системы: проявляются на этапе доступа к компьютеру и обнаружимые после разрешения доступа.

7. По месту расположения в системе: угрозы доступа к информации, находящейся на внешних запоминающих устройствах, в оперативной памяти и к той, что циркулирует в линиях связи.

8. По аспекту ИБ (доступность, целостность, конфиденциальность), против которого направлены угрозы.

Угрозы могут использовать прямой стандартный путь к ресурсам с помощью незаконно полученных паролей или посредством неправомерного применения терминалов законных пользователей, а могут «обойти» существующие средства защиты иным путем. Также необходимо учитывать физическое воздействие на информацию.

В практической деятельности защита информации является комплексом регулярно используемых методов и средств, осуществляемых мероприятий и принимаемых мер для систематического обеспечения нужной надежности информации, которая генерируется, хранится и обрабатывается на объекте, а также передается по каналам.

Защита должна быть системной, т.е. чтобы получить наилучшие результаты, все отдельные виды защиты информации необходимо объединить в одно целое и обеспечить функционирование в составе единой системы, которая представляет собой слаженный механизм взаимодействующих элементов.

Кроме того, комплексная система защиты информации должна обеспечить функционирование надежных механизмов защиты с одной стороны, и управление механизмами защиты информации – с другой. Для этого необходимо предусмотреть организацию отлаженной и четкой системы управления защитой информации.

Таким образом, безопасность в современном информационном мире зависит от предусмотрительности и осведомленности каждого гражданина. Если использовать на практике вышеуказанные рекомендации, то работа в интернет станет намного безопаснее, и пользователи не будут бояться потерять свои личные данные и деньги.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Абаев А.В. Безопасность при работе в сети Интернет / А.В. Абаев // Научное сообщество студентов XXI столетия. Технические науки: сб. ст. по мат. XXXVIII междунар. студ. науч.-практ. конф. № 1(37). – URL: http://sibac.info/archive/technic/1(37).pdf (дата обращения: 10.04.2018).
2. Абраров Р.Д. Информационная безопасность в компьютерных сетях / Р.Д. Абраров, Д.А. Курязов // Молодой ученый. – 2016. – №9.5. – С. 10-12.
3. Алексеев Д.М. Классификация угроз информационной безопасности / Д.М. Алексеев, К.Н. Иваненко, В.Н. Убирайло // Символ науки. – 2016. – №9-1. – С. 18-19.
4. Бабаин С. Инструментарий хакера / С. Бабин. – Спб.: БХВ-Петербург, 2014. – 240 с.
5. Бирюков А.А. Информационная безопасность: защита и нападение / А.А. Бирюков. – М.: ДМК Пресс, 2013. – 474 с.

6. Варлатая С.К. Защита информационных процессов в компьютерных сетях. Учебно-методический комплекс / С.К. Варлатая, М.В. Шаханова. – М.: Проспект, 2015. – 216 с.
7. Галяутдинов Р.Р. Информационная безопасность. Виды угроз и защита информации / Р.Р. Галяутдинов // Сайт преподавателя экономики. – 2014. – URL: http://galyautdinov.ru/post/informacionnaya-bezopasnost (дата обращения: 10.04.2018).
8. Голицына О.Л. Информационные технологии: учебник / О.Л. Голицына, Н.В. Максимов, Т.Л. Партыка, И.И. Попов. – М.: Форум, ИНФРА-М, 2013. – 608 с.
9. Давлетов З.Х. Основы современной информатики: учебное пособие / З.Х. Давлетов. - СПб.: Лань КПТ, 2016. – 256 с.
10. Зверев Г.И. Угрозы и методы обеспечения информационной безопасности виртуальных сред / Г.И. Зверев // Молодой ученый. – 2015. – №9. – С. 235-237.
11. Иванько А.Ф. Информационная безопасность вчера и сегодня / А.Ф. Иванько, М.А. Иванько, А.А. Шанина // Молодой ученый. – 2017. – №51. – С. 25-30.
12. Икон А.И. Компьютерная безопасность в сети / А.И. Икон, Л.В. Васильева // Юный ученый. – 2016. – №2. – С. 80-82.
13. Исаев Г.Н. Информационные технологии: учебное пособие / Г.Н. Исаев. – М.: Омега-Л, 2013. – 464 с.
14. Литвинова А.С. Информационная безопасность, как проблема современного общества / А.С. Литвинова, И.И. Боброва // Портал научно-практических публикаций – URL: http://portalnp.ru/2014/12/2229 (дата обращения: 10.04.2018).
15. Мазаев Д.В. Интернет-угрозы и способы защиты от них / Д.В. Мазаев, В.В. Ермолаева, А.Г. Мурзагалиев // Молодой ученый. – 2015. – №11. – С. 193-197.
16. Максимов Н.В. Современные информационные технологии: учебное пособие / Н.В. Максимов, Т.Л. Партыка, И.И. Попов. – М.: Форум, 2013. – 512 с.
17. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. Стандарт третьего поколения / В.Г. Олифер, Н.А. Олифер. – СПб.: Питер, 2013. – 944 с.
18. Солдатова Г. Интернет: возможности, компетенции, безопасность. Методическое пособие для работников системы общего образования / Г.Солдатова, Е. Зотова, М. Лебешева, В. Шляпников. – М.: Google, 2013. – 165 с.
19. Стариченко Б.Е. Теоретические основы информатики: учебник / Б.Е. Стариченко. – М.: ГЛТ, 2016. – 400 с.
20. Черных Е.А. Анализ классификаций угроз в Интернете / Е.А. Черных // Электронный научно-публицистический журнал «Homo Cyberus». – 2016. – № 1. – URL: http://journal.homocyberus.ru/chernih_e_analis_ugroz_v_internere (дата

обращения: 10.04.2017).

1. Галяутдинов Р.Р. Информационная безопасность. Виды угроз и защита информации / Р.Р. Галяутдинов // Сайт преподавателя экономики. – 2014. – URL: http://galyautdinov.ru/post/informacionnaya-bezopasnost (дата обращения: 10.04.2018). ↑

2. Бирюков А.А. Информационная безопасность: защита и нападение. – М.: ДМК Пресс, 2013. – С. 235. ↑

3. Там же. С.236. ↑

4. Голицына О.Л. Информационные технологии: учебник. – М.: Форум, ИНФРА-М, 2013. – С.208. ↑

5. Абраров Р.Д., Курязов Д.А. Информационная безопасность в компьютерных сетях // Молодой ученый. – 2016. – №9.5. – С. 10. ↑

6. Алексеев Д.М., Иваненко К.Н., Убирайло В.Н. Классификация угроз информационной безопасности // Символ науки. – 2016. – №9-1. – С. 18. ↑

7. Алексеев Д.М., Иваненко К.Н., Убирайло В.Н. Классификация угроз информационной безопасности // Символ науки. – 2016. – №9-1. – С. 18. ↑

8. Там же. С.19. ↑

9. Черных Е.А. Анализ классификаций угроз в Интернете // Электронный научно-публицистический журнал «Homo Cyberus». – 2016. – № 1. – URL: http://journal.homocyberus.ru/chernih_e_analis_ugroz_v_internere (дата обращения: 10.04.2017). ↑

10. Максимов Н.В. Современные информационные технологии: учебное пособие. – М.: Форум, 2013. – С.312. ↑

11. Давлетов З.Х. Основы современной информатики: учебное пособие. - СПб.: Лань КПТ, 2016. – С. 154. ↑

12. Давлетов З.Х. Основы современной информатики: учебное пособие. - СПб.: Лань КПТ, 2016. – С. 155. ↑

13. Мазаев Д.В., Ермолаева В.В., Мурзагалиев А.Г. Интернет-угрозы и способы защиты от них // Молодой ученый. – 2015. – №11. – С. 193. ↑

14. Зверев Г.И. Угрозы и методы обеспечения информационной безопасности виртуальных сред // Молодой ученый. – 2015. – №9. – С. 235. ↑

15. Зверев Г.И. Угрозы и методы обеспечения информационной безопасности виртуальных сред // Молодой ученый. – 2015. – №9. – С. 236. ↑

16. Икон А.И., Васильева Л.В. Компьютерная безопасность в сети // Юный ученый. – 2016. – №2. – С. 80. ↑

17. Икон А.И., Васильева Л.В. Компьютерная безопасность в сети // Юный ученый. – 2016. – №2. – С. 81. ↑

18. Там же. С. 82. ↑

19. Иванько А.Ф., Иванько М.А., Шанина А.А. Информационная безопасность вчера и сегодня // Молодой ученый. – 2017. – №51. – С. 25. ↑

20. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. Стандарт третьего поколения. – СПб.: Питер, 2013. – 944 с. ↑

21. Исаев Г.Н. Информационные технологии: учебное пособие. – М.: Омега-Л, 2013. – С. 234. ↑

22. Стариченко Б.Е. Теоретические основы информатики: учебник. – М.: ГЛТ, 2016. – С.156. ↑

23. Бабаин С. Инструментарий хакера. – Спб.: БХВ-Петербург, 2014. – С.68. ↑

24. Солдатова Г., Зотова Е., Лебешева М., Шляпников В. Интернет: возможности, компетенции, безопасность. Методическое пособие для работников системы общего образования. – М.: Google, 2013. – С.59. ↑

25. Там же. 61. ↑

26. Литвинова А.С., Боброва И.И. Информационная безопасность, как проблема современного общества // Портал научно-практических публикаций – URL: http://portalnp.ru/2014/12/2229 (дата обращения: 10.04.2018). ↑

27. Там же. ↑

28. Литвинова А.С., Боброва И.И. Информационная безопасность, как проблема современного общества // Портал научно-практических публикаций – URL: http://portalnp.ru/2014/12/2229 (дата обращения: 10.04.2018). ↑

29. Литвинова А.С., Боброва И.И. Информационная безопасность, как проблема современного общества // Портал научно-практических публикаций – URL: http://portalnp.ru/2014/12/2229 (дата обращения: 10.04.2018). ↑

30. Галяутдинов Р.Р. Информационная безопасность. Виды угроз и защита информации // Сайт преподавателя экономики. – 2014. – URL: http://galyautdinov.ru/post/informacionnaya-bezopasnost (дата обращения: 10.04.2018). ↑

31. Галяутдинов Р.Р. Информационная безопасность. Виды угроз и защита информации // Сайт преподавателя экономики. – 2014. – URL: http://galyautdinov.ru/post/informacionnaya-bezopasnost (дата обращения: 10.04.2018). ↑

32. Варлатая С.К., Шаханова М.В. Защита информационных процессов в компьютерных сетях. Учебно-методический комплекс. – М.: Проспект, 2015. – С.114. ↑

33. Там же. С. 115. ↑

34. Абаев А.В. Безопасность при работе в сети Интернет // Научное сообщество студентов XXI столетия. Технические науки: сб. ст. по мат. XXXVIII междунар. студ. науч.-практ. конф. № 1(37). – URL: http://sibac.info/archive/technic/1(37).pdf (дата обращения: 10.04.2018). ↑

35. Варлатая С.К., Шаханова М.В. Защита информационных процессов в компьютерных сетях. Учебно-методический комплекс. – М.: Проспект, 2015. – С.116. ↑

36. Там же. С. 117. ↑

37. Варлатая С.К., Шаханова М.В. Защита информационных процессов в компьютерных сетях. Учебно-методический комплекс. – М.: Проспект, 2015. – С.119. ↑