Содержание:

Введение

Актуальность темы данной курсовой работы, заключается в том, что новые информационные технологии активно внедряются в сферу народного пользования. Появление локальных и глобальных сетей представило для пользователей компьютеров новые возможности для оперативного обмена информацией. Но с хранением информации на компьютерных устройствах появляются угрозы конфиденциальности, кражи и целостности информации. По мере развития использования глобальных сетей передачи данных еще больше возросла угроза информационной безопасности из-за возможности ее перехвата во время передачи, а также появления различного вредоносного программного обеспечения.

Под угрозой информационной безопасности понимается совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации. Информационная безопасность — это деятельность по предотвращению утечки персональной информации, несанкционированных и непреднамеренных воздействий на информацию.

Фактор, воздействующий на защищаемую информацию - явление, действие или процесс, результатом которого могут быть утечка, искажение, уничтожение защищаемой информации, блокирование доступа к ней.

Источник угрозы безопасности информации - субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации.

Уязвимость информационной системы (брешь) - свойство информационной системы, обусловливающее возможность реализации угроз безопасности, обрабатываемой в ней информации.

По отношению к информации и информационным ресурсам можно выделить угрозы целостности, конфиденциальности, достоверности и доступности информации, проявляющиеся в различных формах нарушений.

Как правило, вышеперечисленные угрозы информационным ресурсам реализуются следующими способами:

Через имеющиеся агентурные источники в органах государственного управления и коммерческих структурах, имеющих возможность получения конфиденциальной информации (суды, налоговые органы, коммерческие банки и т. д.).

Путем подкупа лиц, непосредственно работающих в организации или структурах, напрямую связанных с ее деятельностью.

Путем перехвата информации, циркулирующей в средствах и системах связи и вычислительной технике с помощью технических средств разведки и съема информации.

Путем прослушивания конфиденциальных переговоров и другими способами несанкционированного доступа к источникам конфиденциальной информации.

Информационная безопасность оказывает влияние на защищенность интересов в различных сферах жизнедеятельности общества и государства. В каждой из них имеются свои особенности обеспечения информационной безопасности, связанные со спецификой объектов обеспечения безопасности, степенью их уязвимости в отношении угроз информационной безопасности.

Цель данной курсовой работы является разобрать основные понятия и виды информационной безопасности, а также рассмотреть стандарты информационной безопасности.

В данной курсовой работе мы разберем, что такое информационная безопасность, кто угрожает информационной безопасности и что должно быть защищено. Приведен анализ угроз информационной безопасности и проблемы аутентификации, секретности, обеспечения целостности и разделение атак.

Помимо этого, будет рассмотрен состав информационной безопасности. Локальная и сетевая безопасность компьютера. А также, конфиденциальность персональных данных, неприкосновенность и доступность данных.

1. Введение в информационную безопасность

1.1 Основные понятия информационной безопасности

Человек волен создавать информацию, но проблема заключается в том, что после создания информации, она перестает быть частью своего владельца и выходит во внешний мир, факт ее независимости является угрозой для ее создателя. Сама по себе информация в защите не нуждается, так как в природе ей ничего не угрожает, трудно представить природные механизмы созданные для уничтожения информации. Информация была, есть и будет, пока существует материя. Но информация, которая принадлежит физическому или юридическому лицу нуждается в защите, потому-что предоставляет для своего собственника ценность. Далеко не каждая информация является реально ценной, но та информация, которая является важной становиться ценностью ее владельца. [1]

Для защиты ценной информации появилась такое направление, как информационная безопасность. Сама по себе информационная безопасность — это защищенность информации, которой располагает ее владелец, от несанкционированного доступа, разрушения и изменения. Информационная безопасность включает в себя меру по защите процессов создания, хранения и обработки информации. Целью информационной безопасности является сохранение информации владельца в целостности и сохранности. [2]

Компьютеризация и развитие технологий предоставляют возможность для хранения персональной информации различного рода. Это могут быть личные фотографии и данные, проекты, книги, схемы, картины находящееся в процессе разработки, данные для осуществления доступа к денежным средствам и так далее. Такая информация имеет прямую ценность для ее владельца и от ее целостности и конфиденциальности зависит, как материальное, так и психологическое состояние ее владельца.

Стоит отметить, что если ранее информация была подвержена краже, через нарушение конфиденциальности, например, несанкционированный доступ к компьютеру, кража пароля от компьютера, намеренное причинение вреда компьютеры, то с развитием глобальной сети Internet, количество угроз только возросло. Это добавило такие понятия, как удаленная кража информации через вредоносное программное обеспечение, такое, как троянские черви, удаленное блокирование компьютера и шифрования данных для денежного вымогания, распространение персональной информации по сети, поломка операционной

системы через вирусы, а также новые формы психологического метода получения персональной информации через фишинг, подставные сайты и письма. [3]

Безусловно, владелец информации понимает, что его информация подвержена риску, ее могут украсть, уничтожить, повредить или изменить. Именно поэтому так актуален в наши дни вопрос защиты информация и информационная безопасность в целом.

Так как информация может пострадать и от кого? Прежде всего информационная безопасность зависит от целостности системы на которой она хранится. Механические повреждения, которые могут повредить компьютер, также повреждают и данные. Это может быть преднамеренное повреждение злоумышленником, непреднамеренное повреждение самим владельцем и природные факторы. Помимо механических повреждений, информационная безопасность зависит от санкционированности доступа к ней, разглашение или несанкционированная передача информации, ошибки в программах и ошибки самих пользователей, а также атаки с использование вредных программ. [4]

Полностью разложить возможные угрозы информационной безопасности лицам, заинтересованным в ее краже и повреждению можно следующим образом:

- Механические повреждения - преднамеренные, например, поджег компьютера конкурентной организацией. Непреднамеренные, например, пролив жидкости на компьютер самим владельцем, что может привести к короткому замыканию. Природные факторы, удар молнии в здание, что может привести к скачку напряжения. Выход из строя оборудования, например, поломка жесткого диска, которая может привести к потере информации;
- Несанкционированный доступ — получение злоумышленником доступа к компьютеру;
- Ошибки пользователя — случайное удаление файлов может привести к потере важной информации;
- Непреднамеренная передача информации — передача пользователем важных данных на фальшивый сайт или почту (фишинг) ;
- Намеренная передача информации — передача данных сотрудником организации конкурентам за различные выгоды;
- Целостность операционной системы — неполадки и ошибки операционной системы или заражения ее вирусом, может привести к потере информации или потери доступа к ней;

- Целостность программного обеспечения — хранения информации в программах или базах данных зависит от ее работоспособности.
- Безопасность сетевого окружения — удаленный доступ к компьютеру, троянские черви, прослушка и кража сегментов данных при передаче угрожают информационной безопасности.

Таким образом, мы получаем целый ряд факторов, которые предоставляют угрозы информационной безопасности. [5]

На основе вышеприведенной информации, можно сделать вывод о том, что безопасность информации находится под высокой угрозой и стоит определить, что должно быть защищено для уменьшения исходящих угроз?

Для начала стоит отметить, что компьютер является средством для обработки информации, диски предназначены для хранения информации, а сети для свободно перемещения информации. Это необходимо понимать, для создания логичной политике безопасности. [6]

На основе этого создадим список объектов, которые должны быть защищены для обеспечения информационной безопасности. Начнем с аппаратной части:

- Центральные процессоры;
- Платы;
- Диски;
- Рабочие Станции;
- Персональный компьютеры;
- Принтеры;
- Дисководы;
- Маршрутизаторы.

Обоснованность этого списка заключается в том, что от корректности работы центрального процессора, платы и дисков зависит целостность информации и ее обработка. Неисправность рабочих станций и персональных компьютеров, может привезти к потере или изменению информации. Не правильно работающие принтеры и дисководы введут к угрозе ввода и вывода информации. От маршрутизаторов зависит целостность при передаче информации по сети.

Вторым список является программное обеспечение:

- Исходные программы;

- Сторонние программы;
- Операционные системы;
- Базы данных.

От правильности работы исходных и сторонних программ зависит целостность информации. Ошибки в работе операционных систем и баз данных могут привести не только к нарушению целостности, но и к полной потере информации.

Создав такой инвентаризационный список можно составить список мер защиты для каждого элемента списка, что приведет к обеспечению информационной безопасности.

Например, чтобы защитить диск компьютера, нужно регулярно производить его диагностику, следить за его рабочими температурами и за работой встроенной технологии самодиагностики S.M.A.R.T. Подключить дополнительный жесткий диск в режиме RAID1. Обеспечить защиту корпуса персонального компьютера от постороннего доступа. Обеспечить подключение компьютера к источнику бесперебойного питания и сетевому фильтру для защиты от скачков напряжения и потери питания. Обеспечить вентилируемость помещения для избегания высокой влажности, которая может привести к окислению контактов жесткого диска. Также защитить само помещение, где находится жесткий диск от несанкционированного доступа. [7]

Все вышеуказанные меры обеспечивают максимальную информационную безопасность для данных, которые хранятся на диске. Если по такому принципу создать меры для защиты каждого элемента в списке, то можно будет обеспечить высокий уровень информационной безопасности.

Можно сделать вывод о степени важности понимания того, что должно быть защищено. Если пропустить один из элементов списка, то это может ослабить защиту других элементов. Например, если не учесть защиту маршрутизатора, то, как бы небыли защищены другие элементы, при передаче информации по сети остается угроза ее целостности.

1.2 Угрозы информационной безопасности

Под угрозой обычно понимается потенциальное возможное явление, которое может привести к нанесению ущерба чьей-то ценности. Угроза информационной

безопасности подразумевает воздействие на нее прямо или косвенно. В настоящее время известен большой перечень угроз информационной безопасности. Рассмотрение потенциальных угроз дает образное представление о том, с каким вызовом сталкивается информационная безопасность. [8]

Классификация возможных угроз информационной безопасности может быть составлена следующим образом:

По природе возникновения:

- естественные угрозы, вызванные объективными физическими процессами или стихийными природными явлениям;
- искусственные угрозы безопасности, вызванные деятельностью человека.

По степени преднамеренности проявления:

- угрозы, вызванные ошибками или халатностью персонала, например, некомпетентное использование средств защиты, ввод ошибочных данных и т.п;
- угрозы преднамеренного действия, например, действия злоумышленников.

По непосредственному источнику угроз:

- природная среда, например, стихийные бедствия, магнитные бури и пр;
- человек, например, вербовка путем подкупа персонала, разглашение конфиденциальных данных и т.д ;
- санкционированные программно-аппаратные средства, например, удаление данных, отказ в работе ОС;
- несанкционированные программно-аппаратные средства, например, заражение компьютера вирусами с деструктивными функциями.

По положению источника угроз:

- не контролируемый зоны, например, перехват данных передаваемых по каналам связи, перехват электромагнитных, акустических и других излучений устройств;
- в пределах контролируемой зоны, например, применение подслушивающих устройств, хищение распечаток, записей, носителей информации и т.п.

По степени воздействия на систему информации:

- вскрытие шифров криптозащиты информации;
- пассивные угрозы, например, угроза копирования секретных данных;
- активные угрозы, например, внедрение троянских коней и вирусов, вносящих изменения в структуру системы.

По степени доступности к данным

- угрозы несанкционированного доступа;
- угрозы некорректного использования;
- несанкционированный доступ, например, незаконное получение паролей и других реквизитов для доступа. ;
- угроза несанкционированного доступа путем использования уязвимостей системы.

По месту расположение информации

- угроза доступа к информации, находящейся на внешних запоминающих устройствах, например, несанкционированное копирование секретной информации с жесткого диска;
- угроза доступа к информации, находящейся в оперативной памяти, чтение остаточной информации и доступ к системе области оперативной памяти путем сторонних прикладных программ;
- угроза доступа к информации в линиях связи, например, незаконное подключение к линии связи, прослушивание каналов, изменение информации, ложные сообщения;
- угроза доступа к информации, отображаемой на терминале или на принтере, например, запись на скрытую видеокамеру. [9]

Угрозы информационной безопасности составляют большой список, помимо угроз, которые связанны из-за намеренного причинения вреда, прямой кражи, природных факторов и т.д., я бы хотел остановиться на угрозе взлома компьютерных систем.

В общем случае программное обеспечение любой универсальной компьютерной системы состоит из трех основных компонентов: операционной системы, сетевого программного обеспечения (СПО) и системы управления базами данных (СУБД). Поэтому все попытки взлома защиты компьютерных систем можно разделить на три группы:

1 атаки на уровне операционной системы;

2 атаки на уровне сетевого программного обеспечения;

3 атаки на уровне систем управления базами данных.

Угроза для СУБД является одной из самых незначительных. Это связано с тем, что СУБД имеют строго определенную внутреннюю структуру, и операции над элементами СУБД заданы довольно четко. Есть четыре основных действия — поиск, вставка, удаление и замена элемента. Другие операции являются вспомогательными и применяются достаточно редко. Наличие строгой структуры и четко определенных операций упрощает решение задачи защиты СУБД. В большинстве случаев злоумышленники предпочитают взламывать защиту компьютерной системы на уровне операционной системы и получать доступ к файлам СУБД с помощью средств операционной системы. Однако в случае, если используется СУБД, не имеющая достаточно надежных защитных механизмов, или плохо протестированная версия СУБД, содержащая ошибки, или если при определении политики безопасности администратором СУБД были допущены ошибки, то становится вполне вероятным преодоление злоумышленником защиты, реализуемой на уровне СУБД.

Угроза операционную системы, в отличие от СУБД, представляет, куда большее значение. Дело в том, что внутренняя структура современных операционных систем чрезвычайно сложна, и поэтому соблюдение адекватной политики безопасности является значительно более трудной задачей.

Нужно просто суметь найти слабое место в конкретной системе защиты. При этом простейшие методы взлома оказываются ничуть не хуже самых изощренных, поскольку, чем проще алгоритм атаки, тем больше вероятность ее завершения без ошибок и сбоев, особенно если возможности предварительного тестирования этого алгоритма в условиях, приближенных к "боевым", весьма ограничены

Успех реализации того или иного алгоритма атаки на практике в значительной степени зависит от архитектуры и конфигурации конкретной операционной системы, являющейся объектом этой атаки. Однако имеются атаки, которым может быть подвергнута практически любая операционная система:

1. кража пароля;

а. подглядывание за пользователем, когда тот вводит пароль, дающий право на работу с операционной системой (даже если во время ввода пароль не высвечивается на экране дисплея, злоумышленник может легко увидеть, пароль,

просто следя за перемещением пальцев пользователя по клавиатуре);

b. получение пароля из файла, в котором этот пароль был сохранен пользователем, не желающим затруднять себя вводом пароля при подключении к сети (как правило, такой пароль хранится в файле в незашифрованном виде);

c. поиск пароля, который пользователи, чтобы не забыть, записывают па календарях, в записных книжках или на оборотной стороне компьютерных клавиатур (особенно часто подобная ситуация встречается, если администраторы заставляют пользователей применять трудно запоминаемые пароли);

d. кража внешнего носителя парольной информации (дискеты или электронного ключа, на которых хранится пароль пользователя, предназначенный для входа в операционную систему);

e. полный перебор всех возможных вариантов пароля;

f. подбор пароля по частоте встречаемости символов и биграмм, с помощью словарей наиболее часто применяемых паролей, с привлечением знаний о конкретном пользователе — его имени, фамилии, номера телефона, даты рождения и т. д., с использованием сведений о существовании эквивалентных паролей, при этом из каждого класса опробуется всего один пароль, что может значительно сократить время перебора.

2. сканирование жестких дисков компьютера (злоумышленник последовательно пытается обратиться к каждому файлу, хранимому на жестких дисках компьютерной системы; если объем дискового пространства достаточно велик, можно быть вполне уверенным, что при описании доступа к файлам и каталогам администратор допустил хотя бы одну ошибку, в результате чего все такие каталоги и файлы будут прочитаны злоумышленником; для сокрытия следов злоумышленник может организовать эту атаку под чужим именем: например, под именем пользователя, пароль которого известен злоумышленник у);

3. сборка "мусора" (если средства операционной системы позволяют восстанавливать ранее удаленные объекты, злоумышленник может воспользоваться этой возможностью, чтобы получить доступ к объектам, удаленным другими пользователями: например, просмотрев содержимое их "мусорных" корзин);

4. превышение полномочий (используя ошибки в программном обеспечении или в администрировании операционной системы, злоумышленник получает полномочия, превышающие полномочия, предоставленные ему согласно действующей политике безопасности);

a. запуск программы от имени пользователя, имеющего необходимые полномочия, или в качестве системной программы (драйвера, сервиса, демона и т. д.);

b. подмена динамически загружаемой библиотеки, используемой системными программами, или изменение переменных среды, описывающих путь к таким библиотекам;

c. модификация кода или данных подсистемы защиты самой операционной системы.

5. отказ в обслуживании (целью этой атаки является частичный или полный вывод из строя операционной системы);

a. захват ресурсов (хакерская программа производит захват всех имеющихся в операционной системе ресурсов, а затем входит в бесконечный цикл);

b. бомбардировка запросами (хакерская программа постоянно направляет операционной системе запросы, реакция на которые требует привлечения значительных ресурсов компьютера);

c. использование ошибок в программном обеспечении или администрировании.

Если в программном обеспечении компьютерной системы нет ошибок и ее администратор строго соблюдает политику безопасности, рекомендованную разработчиками операционной системы, то атаки всех перечисленных пики, малоэффективны. Дополнительные меры, которые должны быть предприняты для повышения уровня безопасности, в значительной степени зависят от конкретной операционной системы, под управлением которой работаем данная компьютерная система. Тем не менее, приходится признать, что вне зависимости от предпринятых мер полностью устранить угрозу взлома компьютерной системы на уровне операционной системы невозможно. Поэтому политика обеспечения безопасности должна проводиться так, чтобы, даже преодолев защиту, создаваемую средствами операционной системы, злоумышленник не смог нанести серьезного ущерба.

Сетевое программное обеспечение является наиболее уязвимым, потому что канал связи, по которому передаются сообщения, чаше всего не защищен, и всякий, кто может иметь доступ к этому каналу, соответственно, может перехватывать сообщения и отправлять свои собственные. Поэтому на уровне СПО возможны следующие атаки:

1. прослушивание сегмента локальной сети (в пределах одного и того же сегмента локальной сети любой подключенный к нему компьютер в состоянии принимать сообщения, адресованные другим компьютерам сегмента, а, следовательно, если компьютер злоумышленник подсоединен к некоторому сегменту локальной сети, то ему становится доступен весь информационный обмен между компьютерами этого сегмента);

2. перехват сообщений на маршрутизаторе (если злоумышленник имеет привилегированный доступ к сетевому маршрутизатору, то он получает возможность перехватывать все сообщения, проходящие через этот маршрутизатор, и хотя тотальный перехват невозможен из-за слишком большого объема, чрезвычайно привлекательным для злоумышленник а является выборочный перехват сообщений, содержащих пароли пользователей и их электронную почту);

3. создание ложного маршрутизатора (путем отправки в сеть сообщений специального вида злоумышленник добивается, чтобы его компьютер стал маршрутизатором сети, после чего получает доступ ко всем проходящим через него сообщениям);

4. навязывание сообщений (отправляя в сеть сообщения с ложным обратным сетевым адресом, злоумышленник переключает на свой компьютер уже установленные сетевые соединения и в результате получает права пользователей, чьи соединения обманным путем были переключены на компьютер злоумышленника);

5. отказ в обслуживании (злоумышленник отправляет в сеть сообщения специальною вида, после чего одна или несколько компьютерных систем, подключенных к сети, полностью или частично выходят из строя).

Подводя итоги, стоит отметить, что защитить компьютер, подключенный к сети от кода злоумышленника невозможно на 100%. В последние годы количество атак использующие слабые места в операционных системах и прикладном программном обеспечении для доступа к информации пользователя, только увеличилось.

Тенденция заключается в том, что код ОС и программного обеспечения расширяется, а вместе с этим появляются узкие места. [10]

Даже создатель одной из самых безопасных операционных систем Linux, Линус Торвальдс сказал следующую фразу:

"Отключите сетевой кабель и создайте "драконовские" условия для обеспечения безопасности, - сказал он. - Вы должны убедиться не только в том, что никто не сможет воспользоваться вашей платформой, но и что никто не хочет это сделать. Это может звучать как крайняя мера, но это очень принципиальный вопрос в области безопасности. Вы не можете смотреть на эти проблемы отдельно от других". [11]

Исходя из этого, можно сделать вывод, что рост угроз информационной безопасности только увеличивается, а классиками пополняется новыми методами угроз. Конечно, существует уголовный кодекс, который защищает и наказывает злоумышленников, которые участвуют в краже и повреждении информации. Поэтому для обеспечения информационной безопасности нужно постоянно изучать материалы о методах ее нарушения и защите, чтобы быть в курсе последних тенденций. Также стоит знать стандарты информационной безопасности. Приложение 1.

1.3 Правовые основы информационной безопасности

Информация является объектом, по поводу которой возникают определенные отношения, имеющие социальное значение и нуждающиеся в регулировании со стороны общества и государства. Это послужило основой для формирования самостоятельной отрасли правовых отношений - информационного права. Одной из форм реализации информационного права является защита информации.

Правовая защита информации - защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по за-щите информации, применение этих документов (актов), а также надзор и контроль за их исполнением.

Поэтому правовая база должна обеспечивать основные функции:

1. Разработка основных принципов отнесения сведений, имеющих конфиденциальный характер, к защищаемой информации;

2. Определение системы органов и должностных лиц, ответственных за обеспечение информационной безопасности в стране и порядка регулирования деятельности предприятий и организаций в этой области;

3. Создание полного комплекса нормативно-правовых руководящих и методических материалов (документов), регламентирующих вопросы обеспечения информационной безопасности как в стране в целом, так и на конкретном объекте;

4. Определение мер ответственности за нарушение правил защиты.

5. Определение порядка разрешения спорных и конфликтных ситуаций по вопросам защиты информации. [12]

В настоящее время основополагающее значение в области информационного права имеют следующие законодательные акты:

Гражданский кодекс Российской Федерации.

Кодекс Российской Федерации об административных правонарушениях.

Доктрина информационной безопасности Российской Федерации от 9 сентября 2000 г. № Пр-1895.

- Федеральный закон № 149-ФЗ от 27 июля 2006 г. «Об инфор¬мации, информационных технологиях и защите информации»;
- Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасно-сти»
- Федеральный закон № 144-ФЗ от 12 августа 1995 г. «Об опера¬тивно-розыскной деятельности»;
- Федеральный закон № 17-ФЗ от 3 февраля 1996 г. «О банках и бан-ковской деятельности»;
- Федеральный закон № 63-ФЗ от 6 апреля 2011 г. «Об электрон¬ной подписи»;
- Федеральный закон № 152-ФЗ от 27 июля 2006 г. «О персональных данных»;
- Федеральный закон № 98-ФЗ от 29 июля 2004 г. «О коммерческой тайне»;
- Федеральный закон № 126-ФЗ от 7 июля 2003 г. «О связи»;
- Федеральный закон № 77-ФЗ от 29 декабря 1994 г. «Об обяза¬тельном экземпляре документов»;
- Федеральный закон № 125-ФЗ от 1 октября 2004 г. «Об архивном де-ле в Российской Федерации»;

- Федеральный закон от 27.07.2010 № 224-ФЗ «О противодействии не-правомерному использованию инсайдерской информации и манипулирова-нию рынком и о внесении изменений в отдельные законодательные акты Рос-сийской Федерации»;
- Закон РФ № 2124-1 от 27 декабря 1991 г. «О средствах массовой ин-формации»;
- Закон РФ № 5485-1 от 21 июля 1993 г. «О государственной тай¬не»;
- Закон РФ № 2124-1 от 27 декабря 1991 г. «О средствах массовой ин-формации»;
- Закон РФ № 5485-1 от 21 июля 1993 г. «О государственной тайне»;
- Закон РФ №176-ФЗ от 24 июня 1999 г. «О почтовой связи»;
- Закон РФ от 11.03.92 г. № 2487-1 «О частной детективной и охранной деятельности». [13]

Защита права на доступ к информации может осуществляться:

- в форме, находящейся за пределами юрисдикции (самозащита своих прав и законных интересов),
- в юрисдикционной форме (в административном или в судебном порядке).

На основе этого существует ответственность за нарушение законодательства в информационной сфере. В **административном порядке** — через подачу жалобы лицом, чьи права нарушены, на должностное лицо (орган) в вышестоящую инстанцию, специальный орган — Судебную палату по информационным спорам при Президенте РФ

В **судебном порядке** — лицо может выбрать любой способ защиты нарушенных прав через подачу иска (жалобы) для рассмотрения в гражданском, административном или уголовном судопроизводстве.

При рассмотрении иска в гражданском судопроизводстве потерпевший вправе использовать основные способы защиты гражданских прав, предусмотренных в статье 12 Гражданского кодекса РФ, в том числе требовать:

- признания права;
- прекращения действий, нарушающих право или создающих угрозу его нарушения;
- признания недействительным акта государственного органа ли органа местного самоуправления;
- восстановления права;

- возмещения убытков;
- компенсации морального ущерба.

Кодекс РФ об административных правонарушениях предусматривает ответственность за административные правонарушения в информационной сфере.

Статья 13.11. Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)

Статья 13.12. Нарушение правил защиты информации

Статья 13.13. Незаконная деятельность в области защиты информации

Статья 13.14. Разглашение информации с ограниченным доступом

Статья 13.15. Злоупотребление свободой массовой информации

Уголовный Кодекс Российской Федерации предусматривает ответственность за информационные преступления.

Статья 138. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений

Статья 140. Отказ в предоставлении гражданину информации

Статья 155. Разглашение тайны усыновления (удочерении)

Статья 183. Незаконное получение и разглашение сведений, составляющих коммерческую или банковскую тайну.

Статья 237. Сокрытие информации об обстоятельствах, создающих опасность для жизни или здоровья людей

Статья 272. Неправомерный доступ к компьютерной информации

Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ.

Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

Статья 275. Государственная измена

Статья 276. Шпионаж [14]

Подводя итоги можно отметить, что информационная безопасность хорошо защищается правовой системой Российской Федерации. Обладатель информации может быть уверен в том, что его информация защищена законом. В свою очередь злоумышленникам приходится брать в расчет то, что их ожидает административная или уголовная ответственность за нарушение информационной безопасности.

2. Обеспечение информационной безопасности компьютера

2.1 Локальная безопасность компьютера

Большинство ранних исследований по компьютерной безопасности было повещено проблеме персонального доступа в системах совместного пользования. В общем случае: если системой пользуется большая группа людей, у каждого из которых есть определенные права использовать определенные программы и видеть определенные данные, то, как мы можем реализовать такие правила контроля доступа?

1. **Конфиденциальность**

Изначально компьютерная безопасность понималась как предотвращение несанкционированного доступа к засекреченной информации. Это предубеждение отчасти развеялось с появлением электронной торговли и практики совершения сделок в Интернете - в этой сфере существенно более важна неприкосновенность. [15]

1. **Неприкосновенность**

Все данные сохраняются в таком виде, в каком они были оставлены последним лицом, правомочным вносить изменения. В контексте компьютерной безопасности «неприкосновенность» означает защиту от записи. Неприкосновенность данных - это гарантия того, что их не удалит и не изменит кто-то, у кого нет на это права. Неприкосновенность программного обеспечения - это гарантия того, что программы не будут изменены по ошибке, по злому умыслу пользователя или

вирусом.

1. **Доступность**

«свойство системы быть готовой и пригодной к работе по требованию законного пользователя».

Совместное обеспечение конфиденциальности, доступности и неприкосновенности сводится к контролю доступа. Суть проблемы состоит в обеспечении законным пользователям возможности делать все то, что им дозволено делать и на что остальные не имеют права.

Существует два способа задать условия контроля доступа: можно оговорить, что разрешено делать различным субъектам, или оговорить, что позволено сделать с разными объектами.

Например, в системе UNIX три вида доступа предоставляют следующие права: читать, писать и выполнять. Все эти права независимы. Например, кто-то, обладающий правом только на чтение файла, не может изменять этот файл. Тот, у кого есть право только на ввод информации, может изменять файл, но не вправе его прочесть. Тот, у кого есть полномочия и на чтение, и на ввод информации, во-лен делать и то и другое. Третий тип права доступа - «выполнять» имеет смысл только для компьютерных программ - исполняемых файлов. [16]

В системе Windows NT более сложный набор прав доступа. В ней предусмотрены права читать, писать и выполнять, а также удалять, изменять права доступа и изменять принадлежность. Владелец файла может разрешить кому-то изменять права доступа к этому файлу или менять его принадлежность.

Сложную систему организации доступа можно представить в виде таблицы. По вертикали расположен список всех возможных пользователей, по горизонтали — список всех файлов. В ячейках таблицы находятся условия доступа пользователя к соответствующему файлу.

В случае компьютерной системы любого разумного размера эта таблица быстро становится очень сложной. Поэтому приходится прибегать к упрощениям.

Один из способов справиться со сложностью контроля доступа состоит в том, чтобы разбить таблицу. В некоторых системах список тех, кто имеет доступ к определенному объекту, хранится вместе с самим объектом. Его часто называют списком контроля доступа (access control list, ACL). Это обычная практика, и ACL

часто используется в целях безопасности операционных систем.

Существует множество теоретических моделей безопасности, разработка многих из них финансировалась Министерством обороны в 70-х и 80-х годах.

Наиболее известна модель Белла-Лападулы - в ней определено большинство понятий, связанных с контролем доступа.

Модель Белла-Лападулы предлагает два основных правила безопасности: одно относится к чтению, а другое - к записи данных. Во-первых, если пользователи имеют категорию допуска «Секретно», то они могут читать несекретные, конфиденциальные и секретные документы, но без права читать совершенно секретные. Во-вторых, если пользователи работают с секретными данными, они могут создавать секретные и совершенно секретные документы, но не могут создавать конфиденциальные и несекретные. [17]

Общее правило звучит так: пользователи могут читать только документы, уровень секретности которых не превышает их допуска, и не могут создавать документы ниже уровня своего допуска. То есть теоретически пользователи могут создавать документы, прочесть которые они не имеют права.

В модели под названием «Китайская стена», например, подробно рассматриваются компьютерные системы, которые работают с данными, полученными от не доверяющих друг другу пользователей, и способы, позволяющие гарантировать каждому из них конфиденциальность.

В модели Кларка-Уилсона центральным является понятие данных, с которыми позволено оперировать только предписанным способом. Например, при помощи этой модели можно реализовать потребности двойной бухгалтерии: каждый кредит необходимо сопоставить равному дебету, и все должно быть записано в специальный аудиторский файл. Эта модель запрещает производить определенные действия без дополнения их другим соответствующим действием: например, запрещено кредитовать счет без записи дебета.

Многие операционные системы имеют встроенные средства безопасности. В этом есть здравый смысл - часто лучше всего поместить средства безопасности на нижних уровнях системы: на аппаратном или уровне операционной системы.

Независимо от того, какая система защиты используется, чаще всего первым шагом работы является идентификация и подтверждение подлинности

(аутентификация).

На самом деле меры контроля доступа должны обеспечить две вещи. Во-первых, пользователь должен попасть в систему, а во-вторых, система должна оставить других снаружи. [18]

Традиционно опознавательные и проверочные меры основываются на чем-то одном из трех: «что вы знаете», «кто вы такой» и «что вам позволено». Это реализуется в виде паролей, биометрических методов распознавания и опознавательных знаков доступа. Иногда системы используют совместно любые две из этих вещей.

Традиционным подходом к проверке подлинности является применение пароля. При входе в операционную систему, первый шаг называется идентификацией (опознаванием): - пользователь сообщает компьютеру свой логин. Второй шаг называется аутентификацией (подтверждением подлинности): пользователь доказывает компьютеру, что он именно тот, кем себя назвал (пароль).

пользователи, как правило, ставят легкие для запоминания пароли, которые легко взломать словарным перебором.

Для решения данной проблемы рекомендуется создание «сильных» паролей. Это означает, что пароли сложней для угадывания и их появление в словаре менее вероятно. Как правило, такие пароли содержат буквы различных регистров, цифры и знаки препинания. [19]

Некоторые системы создают пароли для пользователей случайным образом - путем связывания случайных слогов в произносимое слово.

Также есть биометрическая система проверки. Идея проста: пользователь сам подтверждает свою подлинность: отпечаток голоса, пальцев, глаз и т.д. Данный тип проверки называется биометрическим.

Для большинства методов биометрические данные нужно сохранять в базе данных, как и пароли. [20]

Существует много различных типов биометрических данных: почерк, звучание голоса, узнавание лица, отпечатки пальцев. К биометрикам также относятся линии на руке, сканирование сетчатки, сканирование радужной оболочки глаза, динамические характеристики подписи

Биометрические данные значат очень много, так как на самом деле их сложно подделать: очень трудно нанести ложный отпечаток на свой палец или сделать сетчатку своего глаза похожей на чужую.

Еще одним способом доказательства идентичности является использование чего-либо, что вы имеете: физического опознавательного знака любого рода.

- электронные ключи в номере отеля или ручными - распространенные предметы, предоставляющие доступ в здание.

Также существуют Протоколы аутентификации - это криптографические способы подтверждения подлинности личности.

Основной протокол аутентификации достаточно прост.

1. пользователь набирает свое имя пользователя и пароль на компьютере-клиенте. Клиент отправляет эту информацию серверу;
2. сервер ищет указанное имя пользователя в базе данных и отыскивает соответствующий пароль. Если он соответствует паролю, набранному пользователем, ему предоставляется доступ.

Проблема в том, что база данных паролей должна быть защищена. Решение в том, чтобы хранить не пароли, а хэш-функции паролей.

1. пользователь набирает свое имя пользователя и пароль на клиенте. Клиент отправляет эту информацию серверу;
2. сервер хэширует набранный пользователем пароль;
3. сервер ищет имя пользователя с именем пользователя в базе данных и отыскивает соответствующее хэш-значение. Если это хэш-значение соответствует хэш-значению вновь принятого пароля, ему предоставляется доступ. [21]

Главная проблема со вторым протоколом в том, что пароли открыто посланы по сети. Кто-нибудь, рыскающий по сети, может собирать имена пользователей и пароли. Решение включает в себя хэширование пароля перед тем, как отослать его, но словарные нападения в состоянии справиться и с этим.

Kerberos («Цербер») является более хитрым протоколом аутентификации. Согласно ему, пользователь должен иметь долгосрочный ключ, используемый совместно с надежным сервером в сети, называемым Kerberos-сервером. Чтобы войти во взятый наугад сервер в сети выполняется следующая процедура:

1. пользователь запрашивает разрешение у сервера Kerberos для входа на сервер;
2. сервер Kerberos проверяет, допускается ли пользователь на сервер;
3. сервер Kerberos высылает пользователю «билет», который она обязана отдать серверу, и ключ к сеансу, который используется для доказательства серверу, что это именно тот пользователь;
4. пользователь использует ключ к сеансу с сервера Kerberos для создания «удостоверения», которое он будет использовать, чтобы убедить сервер, что это он;
5. пользователь посылает Бобу и билет, и удостоверение;
6. сервер проверяет. Если все подтверждается, он дает пользователю доступ.

Другие подтверждающие подлинность протоколы входа в систему используют открытые шифровальные ключи. IPsec и SSL, например, пользуются протоколами аутентификации с открытыми ключами.

Вышеуказанные методы обеспечивают высокую локальную безопасность компьютера, но когда дело доходит до сетевого обмена информации, то появляется ряд новых угроз. В таком случае важно обеспечить сетевую безопасность компьютера.

2.2 Сетевая безопасность компьютера

Атаки, организованные через сеть Интернет выделяются в отдельный класс компьютерной безопасности. Они относятся и к компьютерной и сетевой безопасности, но специфика их заключается в использовании сети Интернет. [22]

Самое первое, с чем большинство пользователей сталкивается при первом знакомстве с проблемами компьютерной безопасности — это именно разрушительные программы, то есть программы, умышленно причиняющие неприятности.

К разрушительным программам кроме вирусов относятся так называемые «троянские кони» и «черви». Они обычно состоят из двух частей: «полезной нагрузки» и механизма распространения. «Полезная нагрузка» - это та составляющая, которая, собственно, и вызывает сбои. В некоторых случаях нагрузка способна причинить и большие неприятности: изменить установки контроля доступа компьютера, украсть секретный ключ и отправить его по

электронной почте и т. п. Результат таких действий может оказаться опасным.

Вирусы можно подразделить на три основных класса: файловые вирусы, загрузочные вирусы (вирусы, поражающие загрузочный сектор) и макровирусы. [23]

Долгое время наиболее распространенными были файловые вирусы. Они работали, присоединяясь к программным файлам, например к текстовому редактору или компьютерным играм. При запуске инфицированной программы этот вирус размещается в памяти так, чтобы заразить другие приложения, запускаемые пользователем.

Многие файловые вирусы вымерли после того, как в 1992 году была выпущена Windows 3.1; вирусы просто рушили эту операционную систему и в результате не могли распространяться.

Загрузочные вирусы менее распространены. Эти вирусы размещаются на специальном участке диска (дискеты или жесткого диска), данные с которого загружаются в память при загрузке компьютера. После того как этот вирус внедряется в память, он может заразить соответствующие секторы всех имеющихся жестких Дисков и гибких дисков, вставленных в дисковод, и таким образом распространиться на другие системы. Загрузочные вирусы чрезвычайно эффективны,

Последний класс вирусов — это макровирусы. Они написаны на языке сценариев и заражают не программы, а файлы данных. Во многих текстовых процессорах, электронных таблицах и программах, работающих с базами данных, используются специальные языки разработки сценариев. Такие сценарии (программы на макроязыке, или просто макросы) используются для автоматизации задач и хранятся вместе с данными.

Макровирусы могут распространяться существенно быстрее других, поскольку люди гораздо чаще обмениваются данными, чем программами. А поскольку программное обеспечение электронной почты и передачи файлов делается все проще в обращении, эти вирусы станут распространяться еще быстрее.

Червями называют те разрушительные программы, которые специализируются на компьютерах, подключенных к сети. Это самовоспроизводящиеся программы, которые, в отличие от вирусов, не прячутся в других программах. Они существуют самостоятельно, блуждают по компьютерным сетям, причиняя повреждения.

Роберт Т. Моррис (Robert T. Morris) «выпустил» самого известного червя в 1988 году. Это был интернет-червь, который вывел из строя более 6000 компьютеров: 10% всех серверов Интернета. Червь появлялся на одной машине. Затем он предпринимал попытку проникнуть по сети в другие машины, используя несколько основных приемов. Когда это удавалось, червь засылал на новый компьютер копию своего кода. А затем эта копия повторяла весь процесс, пытаясь проникнуть в очередную машину. Обычно черви работают именно так.

Троянский конь - это код, преднамеренно помещенный в вашу систему, который маскируется под безвредную (или полезную) программу, но делает что-то неожиданное или нежелательное. (С формальной точки зрения код, который вы сознательно размещаете в вашей системе, - это троянский конь, а код, который вводит в вашу систему кто-то другой, называют логической бомбой.) Программист вписывает такой код в крупное программное приложение, которое в результате может начать работать неправильно. [24]

Троянским конем может быть программа, которая тайно устанавливается в компьютере, следит за буфером клавиатуры до тех пор, пока не обнаружит нечто, напоминающее номер кредитной карты, - правильное количество цифр, совпадение контрольной суммы, - и посылает этот номер кому-нибудь при помощи TCP/IP.

HTTP (протокол, используемый в Веб), как и большая часть информации, блуждающей в Интернете, незашифрован и неаутентифицирован. Многие боятся доверять номера своих кредитных карт незашифрованной веб-связи.

Чтобы решить эту проблему, в ранние версии Netscape Navigator включали специальный протокол, так называемый SSL. Этот протокол, который был со временем переименован в TLS, обеспечивает шифрование и аутентификацию веб-связи. SSL довольно хорош, и все его проблемы касаются сертификатов и их применения. Некоторые веб-сайты предоставляют вам возможность выбрать защищенный SSL сеанс связи с браузером. Браузер и веб-сервер применяют шифрование открытым ключом для обмена ключами и симметричное шифрование для кодирования данных. Присутствие в нижней части браузера зеленого ключа или желтого замка дает пользователю возможность почувствовать себя намного свободнее. [25]

На сегодняшний день вирусные программы распространяются крайне быстро, заражая не только компьютеры и сервера, но и мобильные телефоны, что приводит к вирусным эпидемиям, сбоям в работе компаний и многомиллионным убыткам из-

за простоя работы сервисов, утери либо кражи и искажения данных. Очевидно, что в таких обстоятельствах сервера необходимо защищать профессиональным антивирусным программным обеспечением. Большинство антивирусных программ сканируют файлы, выискивая вирусы. В программах есть база данных, содержащая «отпечатки пальцев» вирусов - фрагменты кода, про которые известно, что они являются частью вирусов. Когда программа находит такой же отпечаток, она получает информацию, что файл заражен, и, чтобы «дезинфицировать» его, удаляет вирусный код. Метод сканирования «отпечатков» работает только после того, как компания, создавшая антивирусную программу, выделила вирус в лаборатории и включила в список новый отпечаток.

Благодаря интернету новые типы вирусов распространяются крайне быстро и обнаружение их только лишь по поиску фрагментов и уникального кода (сигнатурам, которые хранятся в базах антивирусных программ) становиться не эффективным.

Самые современные антивирусы используют интеллектуальные методы обнаружения угроз, такие как проактивная защита (эвристика). Таким образом, современный антивирус работает не только понятием «легитимный файл – вредоносный файл», а понятиями «разрешенное действие – запрещенное действие». [26]

Разумеется, методы проактивной защиты не исключают использования классического анализа кода по сигнатурам, а лишь дополняют его. Здесь возникает еще одна проблема при использовании антивирусного ПО: так как количество известных вирусов постоянно растет - увеличивается как снежный ком и размер антивирусных баз с информацией о существующих вирусах.

Производимый "на лету" мониторинг угроз (что является необходимостью) зачастую приводит к существенному замедлению работы компьютеров и серверов. Как показывают результаты тестирований, замедление файловых операций может достигать 100% и более. Чтобы потери в скорости работы вычислительной техники были не столь драматичными, вирусные базы некоторые разработчики периодически "подрезают", - убирая из баз сигнатуры вирусов, которые они считают "устаревшими". Однако тестирования антивирусов, проводимые независимыми организациями (AV-Comparatives.org), показывают, что такие методы оптимизации вредны и могут сделать компьютер беззащитным перед "ретро-вирусом".

Правда это не отменяет важность антивирусного обеспечения. В любом случае антивирус обеспечивает высокий степень защиты информации.

Разговор о безопасности был бы не полным, ведь для защиты информации также существует комплексное программное решение под названием Брандмауэр. Это устройство или программа, предназначенные для фильтрации (разрешения или запрета) сетевой передачи данных, на основании набора правил. Брандмаэр используется для защиты сетей от несанкционированного доступа.

Также, существует другой термин, Фаервол в переводе с англ. Firewall, означает стена огня, в немецком языке. Транскрипция преподнесла другие варианты написания: файерволл, файервол и т.д. имеющие одно и тоже значение. К тому же файервол можно называть межсетевой экран. [27]

В принципе, брандмауэр обеспечивает защиту от хакеров и прочих нападений. Брандмауэр может быть аппаратным средством или программным обеспечением, и действует в качестве сторожа компьютера. Он контролирует весь входящий и исходящий Интернет-трафик.

Брандмауэр просматривает весь трафик на наличие вирусов любого вида:

spyware (шпионское программное обеспечение);

вредоносного программного обеспечения.

Брандмауэр может контролировать Интернет-трафик двумя способами:

фильтрация пакетов;

режим проверки.

Брандмаэур контролирует пакет данных (фильтрация пакетов), который является частью данных, которая содержит адрес своего отправителя и адрес получателя. Этот адрес называется IP. Но что такое IP-адрес? Он действует в качестве определителя для вашего компьютера. IP-адрес - 4-байтовое (32-разрядное) число, задающее уникальный номер компьютеру пользователя в Интернете. Если брандмауэр опознаёт пакет данных и его IP-адрес, то он позволяет этим данным «пройти».

Режим проверки. Этот метод основывается на том, что проверяется часть данных в пакете и сравнивается с большей частью известной и безопасной информации,

если всё оказывается безопасным, то данные поступают на компьютер, если нет, то вход для них блокируется. Этот метод более предпочтителен, так как информация проверяется, прежде чем попасть на компьютер.

Брандмауэр может быть аппаратным, устанавливается на как отдельное устройство и настраивается так, что он работает в качестве двери в вашу сеть. Для работы такого брандмаэура, его следует устанавливать между локальной сетью и интернетом. Преимущество этого метода состоит необходимости для злоумышленника сначала «взломать» брандмаэур, прежде чем получить прямой доступ к любым сетевым ресурсам. Недостаток этого метода заключается в необходимости приобретения дополнительных аппаратных средств. Иногда аппаратным брандмаэуром называют отдельный компьютер, выделенный специально для этих целей. На него устанавливается необходимое программное обеспечение и две сетевые карты (одна «смотрит» в вашу сеть, другая – в сеть интернет). В данном случае, вам достаточно будет низко производительного компьютера, так как обычно программное обеспечение не требовательно к ресурсам.

Программным брандмаэуром называется программное обеспечение, устанавливаемое на компьютер, который необходимо защитить от сетевых угроз. Преимущества этого типа заключаются в более простой настройке и в отсутствии дополнительного оборудования. Недостатки программных брандмаэуров заключены в том нерадостном факте, что они занимают системные ресурсы, и их необходимо устанавливать на всех рабочих станциях и серверах сети. [28]

Теперь, когда мы разобрали что такое брандмауэр стоит отметить, что все современные операционные системы поставляются с программными брандмаэурами, которые по умолчанию уже установлены. Тем не менее, если у пользователя есть желание попробовать другой программный брандмауэр, то он сможет найти их великое множество.

Хоть и по мере развития сетевых технологий и сетевой передачи данных появляются все больше угроз, появляются новые методы защиты информационной безопасности, защищенные протоколы, шифрование, а также антивирусы и брендмауэры, которые успешно противостоят угрозам безопасности информации в сети. Важно отметить то, что для повышения информационной безопасности следует обеспечить правильную политику безопасности для пользователей, а также регулярно обновлять и следить за работой антивирусов и брендмаэров.

Заключение

Информационная безопасность относится к числу направлений деятельности, развивающихся чрезвычайно быстрыми темпами. Этому способствуют как общий прогресс информационных технологий, так и постоянное противоборство между желающими добыть конфиденциальную информацию и желающими ее сохранить.

В данной курсовой работе, в первой главе были изложены основные понятия информационной безопасности, на примерах описаны примеры угроз и лица, которые могут ими воспользоваться. Детали компьютерной системы, которые нужно защитить для обеспечения информационной безопасности. Также была описана детальная классификация угроз. Рассмотрена угроза взлома компьютерных систем. А также рассмотрены правовые основы информационной безопасности.

Во второй главе было уделено внимание обеспечению локальной и сетевой безопасности компьютера.

По мере расширения технологий хранения персональной информации, появляются новые уязвимости, которые могут быть использованы злоумышленниками. Но по мере обнаружения новых угроз информационной безопасности, пополняется классификация, создаются новые способы защиты и стандарты.

Помимо этого, существует правовая база, направленная на защиту обладателей ценной информации и на наказание злоумышленников, которые пытаются ее добыть или навредить информации другой личности.

Опыт показывает, что для достижения эффективных решений по защите информации необходимо сочетание правовых, организационных и технических мероприятий. То есть обеспечение защиты информации и в целом информационной безопасности современных информационных систем требует комплексного подхода. Оно невозможно без применения широкого спектра защитных средств, объединенных в продуманную архитектуру

На основе изложенного материала можно заключить, что информационная безопасность имеет большое значение, а ее актуальность постоянно увеличивается, по мере развития информационных технологий.

Библиография

1. Вихорев Сергей Викторович Директор департамента ОАО «Элвис Плюс» - КЛАССИФИКАЦИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ URL:http://www.cnews.ru/reviews/free/oldcom/security/elvis_class.shtml
2. ARinteg - Виды угроз информационной безопасности URL:http://www.arinteg.ru/articles/ugrozy-informatsionnoy-bezopasnosti-27123.html
3. Шабуров А.С. - Информационная безопасность предприятия / Шубаров А.С.: Изд-во «Пермь» 2011 – 68 с.
4. В.Ф. Шаньгин — Информационная безопасность компьютерных систем и сетей / В.Ф. Шаньгин: Изд-во «ФОРУМ» 2011. - 416 с.
5. Э.Н. Камышев — Информационная безопасность и защита информации / Э.Н. Камышев: Изд-во «Томск» 2009. - 95 с.
6. Бакланов В В - Введение в информационную безопасность. Направления информационной защиты / Бакланов В В: Изд-во «УрФу» 2012. - 235 с.
7. Бирюков А.А. - Информационная безопасность. Защита и нападение / Бирюков А.А.: Изд-во «ДМК Пресс» 2012. - 474 с.
8. Садердинов А.А., Трайнев В.А., Федулов А.А. - Информационная безопасность предприятия / Садердинов А.А., Трайнев В.А., Федулов А.А.: Изд-во «Дашков и К» 2005. - 301 с.
9. Рассел Р. - Защита от хакеров корпоративных сетей / Рассел Р.: Изд-во «ДМК Пресс» 2005. - 553 с.
10. Скотт Бармен - Разработка правил информационной безопасности / Скотт Бармен: Изд-во «Вильям» 2002. - 200 с.

Приложение 1

Отечественные и зарубежные стандарты в области

информационной безопасности

1. ГОСТ 28147—89, «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования»;
2. ГОСТ Р 34.10—94, «Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма»;
3. ГОСТ Р 34.11-94, «Информационная технология. Криптографическая защита информации. Функция хэширования»;

4. ГОСТ Р 50739-95, «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования»
5. ГОСТ Р 50922-2006 Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения;;
6. ГОСТ Р 51275-99 «Объект информатизации. Факторы, воздействующие на информацию»;
7. ГОСТ Р 50949 – 2001. «Средства отображения информации индивидуального пользования. Методы применения и оценки эргономических параметров безопасности»;
8. ГОСТ Р ИСО/МЭК 15408 -1 – 2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. ч.1: Введение и общая модель»;
9. ГОСТ Р ИСО/МЭК 15408 -2 – 2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. ч.2: Функциональные требования безопасности»;
10. ГОСТ Р ИСО/МЭК 15408 -2 – 2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. ч.3: Требования доверия к безопасности»;
11. ГОСТ Р 51897 – 2002 «Менеджмент риска. Термины и определения.

Данные ГОСТы относятся к различным группам по классификатору стандартов. Кроме того, есть семейства родственных стандартов, имеющих отношение к области защиты информации можно отнести:

- системы тревожной сигнализации, комплектуемые изъвещателями различного принципа действия, — 12 ГОСТов;
- информационные технологии (сертификация систем телекоммуникации, программных и аппаратных средств, аттестационное тестирование взаимосвязи открытых систем, аттестация баз данных и т. д.) - около 200 ГОСТов;
- системы качества (в том числе стандарты серии 9000, введенные в действие на территории РФ) — больше 100 ГОСТов.

1. Бирюков А.А. - Информационная безопасность. Защита и нападение / Бирюков А.А.: Изд-во «ДМК Пресс» 2012. - С.64 ↑

2. Садердинов А.А., Трайнев В.А., Федулов А.А. - Информационная безопасность предприятия / Садердинов А.А., Трайнев В.А., Федулов А.А.: Изд-во «Дашков и К» 2005. - С. 4 ↑

3. В.Ф. Шаньгин — Информационная безопасность компьютерных систем и сетей / В.Ф. Шаньгин: Изд-во «ФОРУМ» 2011. - С.9 ↑

4. Скотт Бармен - Разработка правил информационной безопасности / Скотт Бармен: Изд-во «Вильям» 2002. - С. 24 ↑

5. Рассел Р. - Защита от хакеров корпоративных сетей / Рассел Р.: Изд-во «ДМК Пресс» 2005. - С. 11 ↑

6. Скотт Бармен - Разработка правил информационной безопасности / Скотт Бармен: Изд-во «Вильям» 2002. - С. 26 ↑

7. Бакланов В В - Введение в информационную безопасность. Направления информационной защиты / Бакланов В В: Изд-во «УрФу» 2012. – С. 122 ↑

8. В.Ф. Шаньгин — Информационная безопасность компьютерных систем и сетей / В.Ф. Шаньгин: Изд-во «ФОРУМ» 2011. – С.16 ↑

9. ARinteg - Виды угроз информационной безопасности URL:http://www.arinteg.ru/articles/ugrozy-informatsionnoy-bezopasnosti-27123.html ↑

10. Рассел Р. - Защита от хакеров корпоративных сетей / Рассел Р.: Изд-во «ДМК Пресс» 2005. – С. 16 ↑

11. Заявление Линуса Товарльдса - http://4pda.ru/2015/09/27/247855/ ↑

12. Э.Н. Камышев — Информационная безопасность и защита информации / Э.Н. Камышев: Изд-во «Томск» 2009. – С. 31 ↑

13. Официальный интернет-портал правовой информации - http://pravo.gov.ru/ ↑

14. Официальный интернет-портал правовой информации - http://pravo.gov.ru/ ↑

15. Бирюков А.А. - Информационная безопасность. Защита и нападение / Бирюков А.А.: Изд-во «ДМК Пресс» 2012. – С.122 ↑

16. Садердинов А.А., Трайнев В.А., Федулов А.А. - Информационная безопасность предприятия / Садердинов А.А., Трайнев В.А., Федулов А.А.: Изд-во «Дашков и К» 2005. – С. 46 ↑

17. Бакланов В В - Введение в информационную безопасность. Направления информационной защиты / Бакланов В В: Изд-во «УрФу» 2012. – С. 187 ↑

18. Садердинов А.А., Трайнев В.А., Федулов А.А. - Информационная безопасность предприятия / Садердинов А.А., Трайнев В.А., Федулов А.А.: Изд-во «Дашков и К» 2005. - 301 с. ↑

19. Скотт Бармен - Разработка правил информационной безопасности / Скотт Бармен: Изд-во «Вильям» 2002. - 200 С. 73 ↑

20. Садердинов А.А., Трайнев В.А., Федулов А.А. - Информационная безопасность предприятия / Садердинов А.А., Трайнев В.А., Федулов А.А.: Изд-во «Дашков и К» 2005. – С. 89 ↑

21. Скотт Бармен - Разработка правил информационной безопасности / Скотт Бармен: Изд-во «Вильям» 2002. – С. 176 ↑

22. В.Ф. Шаньгин — Информационная безопасность компьютерных систем и сетей / В.Ф. Шаньгин: Изд-во «ФОРУМ» 2011. - 416 с. ↑

23. Бакланов В В - Введение в информационную безопасность. Направления информационной защиты / Бакланов В В: Изд-во «УрФу» 2012. – С. 198 ↑

24. В.Ф. Шаньгин — Информационная безопасность компьютерных систем и сетей / В.Ф. Шаньгин: Изд-во «ФОРУМ» 2011. – С. 46 ↑

25. Рассел Р. - Защита от хакеров корпоративных сетей / Рассел Р.: Изд-во «ДМК Пресс» 2005. – С. 133 ↑

26. Садердинов А.А., Трайнев В.А., Федулов А.А. - Информационная безопасность предприятия / Садердинов А.А., Трайнев В.А., Федулов А.А.: Изд-во «Дашков и К» 2005. – С. 56 ↑

27. В.Ф. Шаньгин — Информационная безопасность компьютерных систем и сетей / В.Ф. Шаньгин: Изд-во «ФОРУМ» 2011. – С. 193 ↑

28. Бирюков А.А. - Информационная безопасность. Защита и нападение / Бирюков А.А.: Изд-во «ДМК Пресс» 2012. – С.277 ↑