Содержание:

Введение

Цель курсовой работы – определение основные виды угроз, существующие методы и средства защиты информации, определить сущность информационной безопасности.

Под безопасностью информации понимается защищенность системы от случайного или преднамеренного вмешательства в нормальный процесс ее функционирования и попыток хищения. 21 век знаменуется бурным развитием информационных технологий. Информация в большей мере становится стратегическим ресурсом, дорогим товаром и производительной силой. Одним из важнейших аспектов проблемы обеспечения информационной безопасности является определение, анализ и классификация возможных угроз безопасности информации.
Анализ каналов утечки информации в информационной системе предприятий.

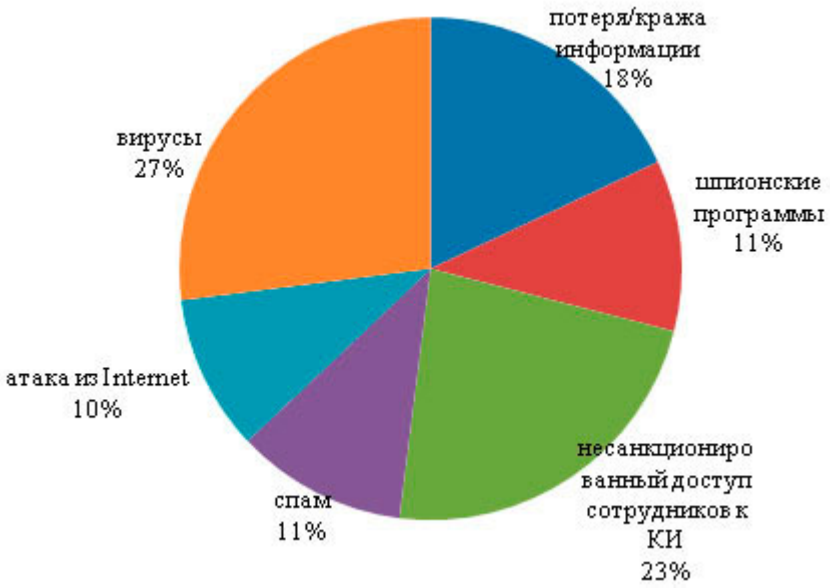

Рисунок 1. Основные виды угроз информационной безопасности

Информация, подобно любым другим существующим товарам, также нуждается в своей сохранности и надежной защите. Одна из наиболее острых проблем – информационная безопасность, которую необходимо обеспечивать, контролировать, а также создавать условия для ее управления.

Информационная безопасность — это защищенность информации и соответствующей инфраструктуры от случайных или преднамеренных воздействий сопровождающихся нанесением ущерба владельцам или пользователям информации. Защищенности информационных ресурсов от незаконного ознакомления, преобразования и уничтожения, воздействий направленных на нарушение их работоспособности. Информационная безопасность достигается обеспечением конфиденциальности, целостности и достоверности обрабатываемых данных, а также доступности и целостности информационных компонентов и ресурсов.

Информационная безопасность достигается проведением руководством соответствующего уровня политики информационной безопасности. В программах, которой содержатся общие требования и принцип построения систем защиты информации.

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

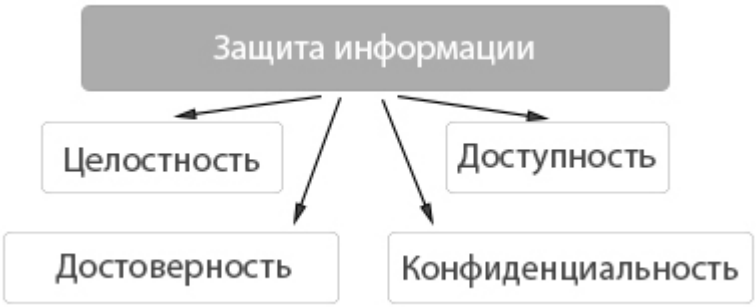

Рисунок 1. Защита информации.

Под конфиденциальностью подразумевают необходимость введения ограничения доступа к данной информации для определенного круга лиц, гарантия, что в процессе передачи данные могут быть известны только легальным пользователям.

Целостность – это свойство информации сохранять свою структуру и/или содержание в процессе передачи и хранения в неискаженном виде по отношению к некоторому фиксированному состоянию. Информацию может создавать, изменять или уничтожать только авторизованное лицо (законный, имеющий право доступа пользователь).

Достоверность – это свойство информации, выражающееся в строгой принадлежности субъекту, который является ее источником, либо тому субъекту, от которого эта информация принята.

Доступность – это свойство информации, характеризующее способность обеспечивать своевременный и беспрепятственный доступ пользователей к необходимой информации.

Глава 1. «угроза информационной безопасности»

Понятие угрозы информационной безопасности раскрыто в целом ряде законодательных актов РФ, Стандартов (ГОСТ) РФ и руководящих документах ФСБ РФ и ФСТЭК России.

Угроза безопасности – совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства. (Закон Российской Федерации «О безопасности»)

Угроза: Потенциальная причина инцидента, который может нанести ущерб системе или организации. (ГОСТ Р ИСО/МЭК ТО 13335-1)

Угроза (безопасности информации): совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации. (ГОСТ Р 50922-2006)

Под угрозой безопасности информации понимаются события или действия, которые могут привести к искажению, несанкционированному использованию или даже к разрушению информационных ресурсов управляемой системы, а также программных и аппаратных средств.

Если исходить из классического рассмотрения кибернетической модели любой управляемой системы, возмущающие воздействия на нее могут носить случайный характер.

Основные виды угроз информационной безопасности:

- стихийные бедствия и аварии (наводнение, ураган, землетрясение, пожар и т.п.);

- сбои и отказы оборудования (технических средств) автоматизированных систем;

- последствия ошибок проектирования и разработки компонентов) автоматизированных систем (аппаратных средств, технологии обработки информации, программ, структур данных и т.п.);

- ошибки эксплуатации (пользователей, операторов и другого персонала);

преднамеренные действия нарушителей и злоумышленников (обиженных лиц из числа персонала, преступников, шпионов, диверсантов и т.п.).

Глава 2. «классификация угроз безопасности»

Утечка по странам согласно мониторинга компании InfoWatch:

Рисунок 3. Анализ утечки по странам в период 2010-2015г.

По природе возникновения различают:

2.1 Естественные угрозы

Угрозы, вызванные воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека.

Примеры естественных угроз

- пожар. Поэтому при проектировании автоматизированных систем целесообразно рассмотреть вопросы противопожарной безопасности.

- затопление. В этих случаях аппаратные средства автоматизированных систем целесообразно устанавливать на верхних этажах зданий и должны приниматься другие меры предосторожности.

- стихийного бедствия. Ущерб может быть нанесен при технических авариях, например, при внезапном отключении электропитания и т.д.

2.2 Искусственные угрозы

Угрозы, вызванные деятельностью человека. Среди них, исходя из мотивации действий, можно выделить:

- непреднамеренные (неумышленные, случайные)
Угрозы вызванные ошибками в проектировании автоматизированных систем и ее элементов, ошибками в программном обеспечении, ошибками в действиях персонала и т.п.;
Основные непреднамеренные искусственные угрозы автоматизированных систем. Действия, совершаемые людьми случайно, по незнанию, невнимательности или халатности, из любопытства, но без злого умысла:

- неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы (неумышленная порча оборудования, удаление, искажение файлов с важной информацией или программ, в том числе системных и т.п.);

- неправомерное отключение оборудования или изменение режимов работы устройств и программ;

- неумышленная порча носителей информации;

- запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы (зависания или зацикливания) или осуществляющих необратимые изменения в системе (форматирование или реструктуризацию носителей информации, удаление данных и т.п.);

- нелегальное внедрение и использование неучтенных программ (игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения нарушителем своих служебных обязанностей) с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях);

- заражение компьютера вирусами;

- неосторожные действия, приводящие к разглашению конфиденциальной информации, или делающие ее общедоступной;

- разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.);

- проектирование архитектуры системы, технологии обработки данных, разработка прикладных программ, с возможностями, представляющими опасность для работоспособности системы и безопасности информации;

- игнорирование организационных ограничений (установленных правил) при работе в системе;

- вход в систему в обход средств защиты (загрузка посторонней операционной системы со сменных магнитных носителей и т.п.);

- некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом службы безопасности;

- пересылка данных по ошибочному адресу абонента (устройства);

- ввод ошибочных данных;

- неумышленное повреждение каналов связи.

2.3 преднамеренные (умышленные)

Угрозы связанные с корыстными устремлениями людей-злоумышленников.

Источники угроз по отношению к автоматизированным системам могут быть внешними или внутренними.

Основные преднамеренные искусственные угрозы

Основные возможные пути умышленной дезорганизации работы, вывода системы из строя, проникновения в систему и несанкционированного доступа к информации:

- физическое разрушение системы (путем взрыва, поджога и т.п.) или вывод из строя всех или отдельных наиболее важных компонентов компьютерной системы (устройств, носителей важной системной информации, лиц из числа персонала и т.п.);

- отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, охлаждения и вентиляции, линий связи и т.п.);

- действия по дезорганизации функционирования системы (изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных радиопомех на частотах работы устройств системы и т.п.);

- внедрение агентов в число персонала системы (в том числе, возможно, и в административную группу, отвечающую за безопасность);

- вербовка (путем подкупа, шантажа и т.п.) персонала или отдельных пользователей, имеющих определенные полномочия;

- применение подслушивающих устройств, дистанционная фото- и видеосъемка и т.п.;

- перехват побочных электромагнитных, акустических и других излучений устройств и линий связи, а также наводок активных излучений на вспомогательные технические средства, непосредственно не участвующие в обработке информации (телефонные линии, сети питания, отопления и т.п.);

- перехват данных, передаваемых по каналам связи, и их анализ с целью выяснения протоколов обмена, правил вхождения в связь и авторизации пользователя и последующих попыток их имитации для проникновения в систему;

- хищение носителей информации (магнитных дисков, лент, микросхем памяти, запоминающих устройств и целых ПЭВМ);

- несанкционированное копирование носителей информации;

- хищение производственных отходов (распечаток, записей, списанных носителей информации и т.п.);

- чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;

- чтение информации из областей оперативной памяти, используемых операционной системой (в том числе подсистемой защиты) или другими пользователями, в асинхронном режиме используя недостатки мультизадачных операционных систем и систем программирования;

- незаконное получение паролей и других реквизитов разграничения доступа (агентурным путем, используя халатность пользователей, путем подбора, путем имитации интерфейса системы и т.д.) с последующей маскировкой под зарегистрированного пользователя ("маскарад");

- несанкционированное использование терминалов пользователей, имеющих уникальные физические характеристики, такие как номер рабочей станции в сети, физический адрес, адрес в системе связи, аппаратный блок кодирования и т.п.;

- вскрытие шифров криптозащиты информации;

- внедрение аппаратных спецвложений, программных "закладок" и "вирусов" ("троянских коней" и "жучков"), то есть таких участков программ, которые не нужны для осуществления заявленных функций, но позволяющих преодолевать систему защиты, скрытно и незаконно осуществлять доступ к системным ресурсам с целью регистрации и передачи критической информации или дезорганизации функционирования системы;

- незаконное подключение к линиям связи с целью работы "между строк", с использованием пауз в действиях законного пользователя от его имени с последующим вводом ложных сообщений или модификацией передаваемых сообщений.

Утечка информации согласно мониторинга компании InfoWatch:

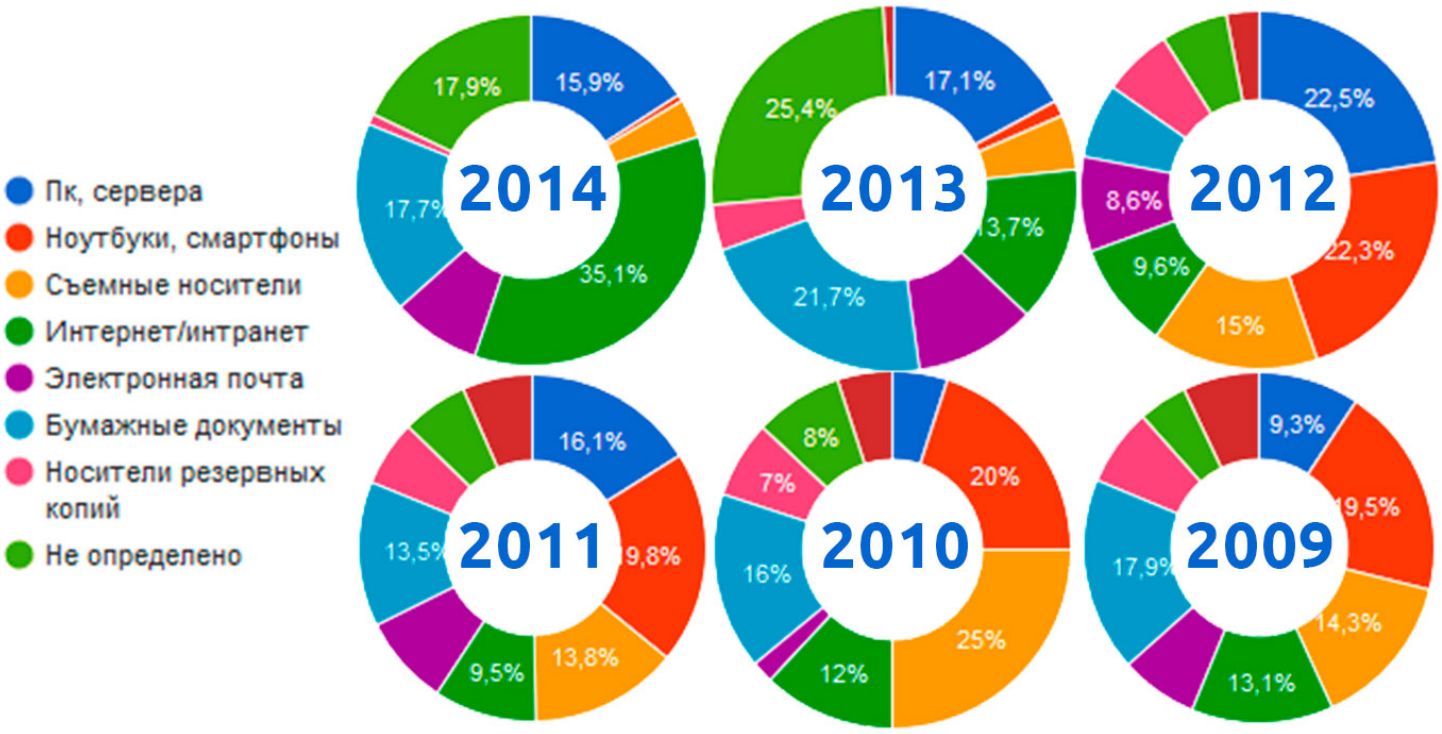

Рисунок 4. Каналы утечек в период 2009-2014г.

Глава 3. «виды угроз»

По отношению к отдельной организации существуют следующие основные виды внешних угроз:

- Недобросовестные конкуренты.

- Криминальные группы и формирования.

- Противозаконные действия отдельных лиц и организаций административного аппарата, в том числе и налоговых служб.

- Нарушение установленного регламента сбора, обработки и передачи информации.

Основные виды внутренних угроз:

- Преднамеренные преступные действия собственного персонала организации.

- Непреднамеренные действия и ошибки сотрудников.

- Отказ оборудования и технических средств.

- Сбои программного обеспечения средств обработки информации.

Внутренние и внешние угрозы тесно взаимодействуют. Соотношение внутренних и внешних угроз в соответствии с характеризуется следующими показателями: 81,7% угроз совершается либо самими сотрудниками организаций, либо при их прямом или опосредованном участии (внутренние угрозы); 17,3% угроз — внешние угрозы или преступные действия; 1,0% угроз — угрозы со стороны случайных лиц.

Согласно данным мониторинга компании InfoWatch (занимающейся разработкой решений для защиты бизнеса от внутренних угроз информационной безопасности) количество утечек информации постоянно увеличивается (например, в 2015 на 22 %) .

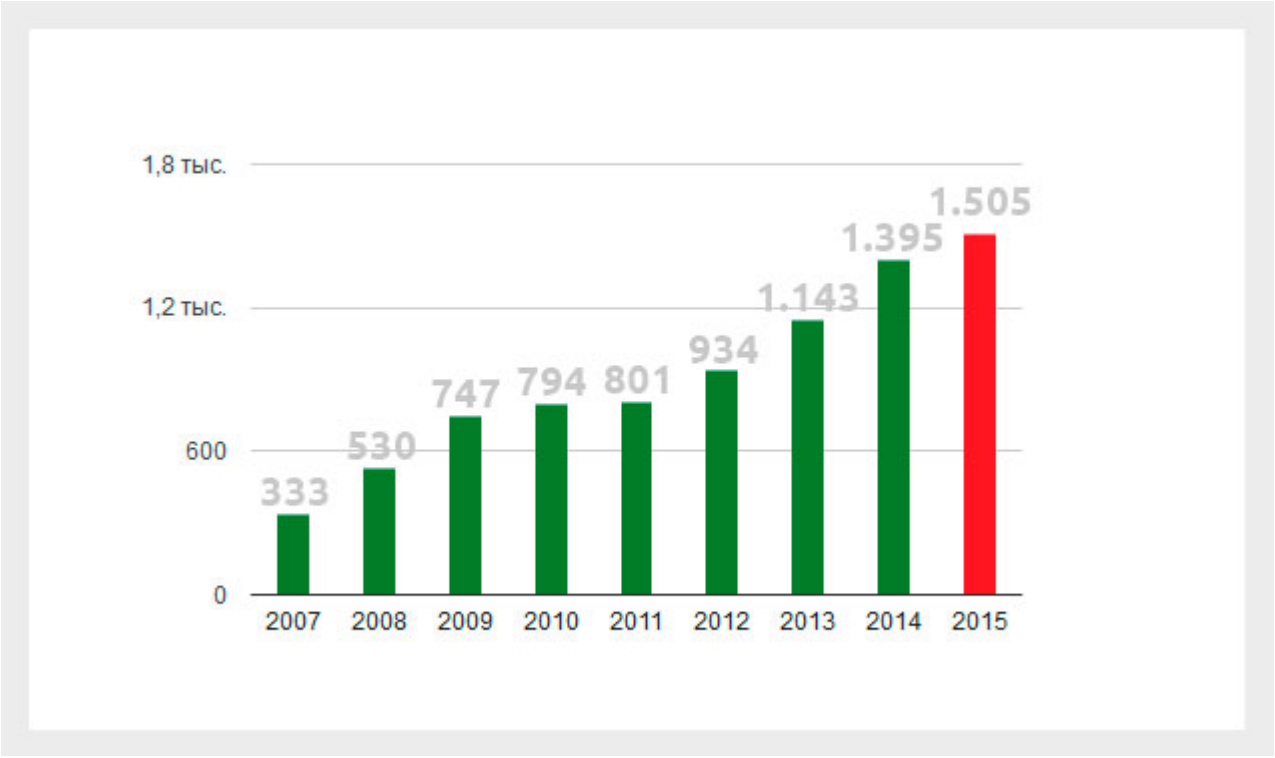

Рисунок 5. Рост числа утечек в мире.

Это вызывает опасения еще и потому, что большая часть утечек информации (92%) относятся к персональным данным. Причем соотношение умышленных и неумышленных инцидентов практически равно.

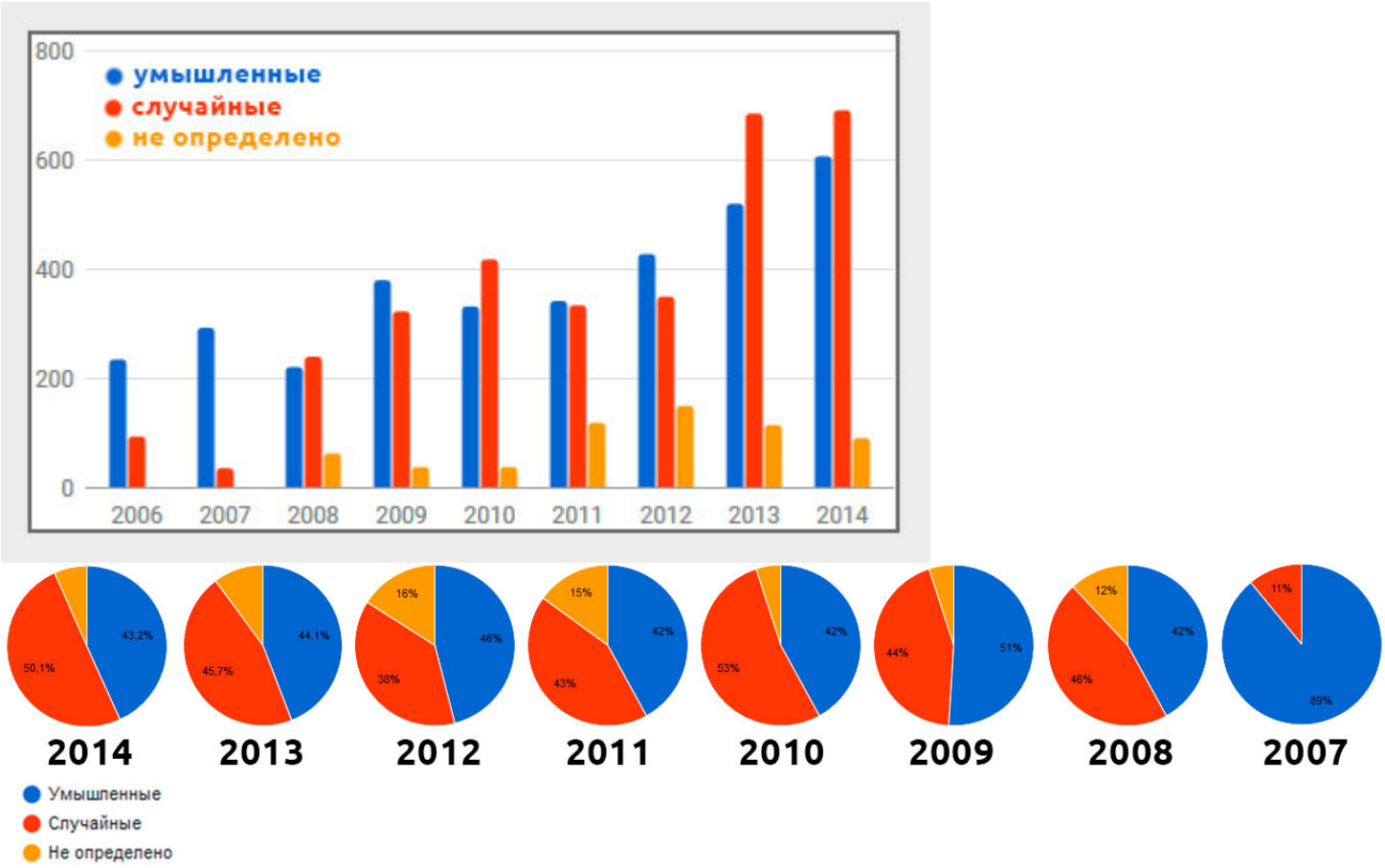

Рисунок 6. Соотношение умышленных и неумышленных утечек.

Внешние угрозы и целевые атаки:

Целевые атаки – это заранее спланированные действия по атаке на IT-системы конкретной организации. У каждой атаки есть заказчик, исполнитель, объект-жертва и цель.

Отличие целевых атак от вирусов:

- Использование нескольких векторов нападения одновременно
- Использование методов социальной инженерии

Социальная инженерия – это метод несанкционированного доступа к информации, основанный на использовании слабостей человеческого фактора и без использования технических средств. Злоумышленник получает информацию, например, с помощью обычного телефонного звонка или путем проникновения в организацию под видом ее служащего.

- Заранее произведена «разведка» – получена информация об инфраструктуре предприятия, используемых методах и средствах защиты

- Как правило, происходит отключение используемой защиты
- Часто целевая атака начинается с DDoS-атаки

DDoS-атака (Distributed Denial of Service) – это атака на веб-ресурс, основной целью которой является выведение его из строя путем подачи большого количества ложных запросов, которые сервер не успевает обрабатывать, и сайт становится недоступным для пользователя.

- Вредоносный код, как правило, внедряется по частям

В основном защита осуществляется техническими средствами:

- Антивирусы (Kaspersky, Symantec, G DATA и др.)
- Защитные сетевые экраны (Entensys, Kerio и др.)
- Специализированные средства защиты от DDoS (Attack Killer, Qrator и др.)
- Технологии защиты от уязвимостей (Appercut, Checkmarx, Fortify и др.)
- Специализированные средства по защите от целевых атак (Attack Killer, FireEye и др.)

Правильнее всего выстраивать эшелонированную защиту, используя технологии от различных производителей. Это резко усложняет задачу атакующего.

Утечки через мобильные устройства:

Современные смартфоны передают на сторону

информацию о пользователе:

- определение местонахождения

- содержание переписки (смс, почта)

- фото- и видеофайлы

- контакты

- связь с браузерами и поисковиками на десктопах

- анализ предпочтений пользователей

(политические взгляды, потребительские привычки, личная жизнь)

- все возможности слежки от поисковиков, соцсетей, браузеров, операционной системы

Смартфоны имеют дополнительную встроенную батарею, поэтому даже в выключенном состоянии могут передавать информацию.

Информационные атаки – это кампании очернения и подрыва репутации

предприятия с помощью современных электронных СМИ и соцсетей.

Часто такие кампании служат средством конкурентной борьбы.

Виды информационных атак:

Атаки на руководство

- «Раскрутка» неудачных высказываний руководителей или учредителей

организаций

- Вбросы и раскрутка информации о происшествиях, неудачных решениях,

поступках или благосостоянии

- Клевета в отношении руководителей или учредителей организаций

Атаки на предприятие

- Вбросы и раскрутка информации о сбоях и ошибках на предприятии

Длительные кампании очернения

- Серии вбросов

- Подбор негативных тем, вызывающих живой отклик и вирусный рост

- Подогревание темы в течение многих месяцев

Важно понимать, что нет неуязвимых систем. Главное – сделать атаку на вашу систему слишком дорогой и сложной для атакующих.

Глава 4. «неформальная модель нарушителя»

Типичный компьютерный преступник - это не молодой хакер, использующий

телефон и домашний компьютер для получения доступа к большим компьютерам. Типичный компьютерный преступник - это служащий, которому разрешен доступ к системе, нетехническим пользователем которой он является.

Определение 2. Нарушитель - это лицо, предпринявшее попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или удовольствия, с целью самоутверждения и т.п.) и использующее для этого различные возможности, методы и средства.

Злоумышленником – это нарушитель, намеренно идущий на нарушение из корыстных побуждений.

Неформальная модель нарушителя отражает его практические и теоретические возможности, время и место действия и т.п. Для достижения своих целей нарушитель должен приложить некоторые усилия, затратить определенные ресурсы. Исследовав причины нарушений, можно либо повлиять на сами эти причины (конечно если это возможно), либо точнее определить требования к системе защиты от данного вида нарушений или преступлений.

В каждом конкретном случае, исходя из конкретной технологии обработки информации, может быть определена модель нарушителя, которая должна быть адекватна реальному нарушителю для данной автоматизированной системы.

При разработке модели нарушителя определяются:

• предположения о категориях лиц, к которым может принадлежать нарушитель;

• предположения о мотивах действий нарушителя (преследуемых нарушителем целях);

• предположения о квалификации нарушителя и его технической оснащенности (об используемых для совершения нарушения методах и средствах);

• ограничения и предположения о характере возможных действий нарушителей.

По отношению к автоматизированным системам нарушители могут быть внутренними (из числа персонала системы) или внешними (посторонними лицами). Внутренним нарушителем может быть лицо из следующих категорий персонала:

• пользователи (операторы) системы;

• персонал, обслуживающий технические средства (инженеры, техники);

• сотрудники отделов разработки и сопровождения ПО (прикладные и системные программисты);

• технический персонал, обслуживающий здания (уборщики, электрики, сантехники и другие сотрудники, имеющие доступ в здания и помещения, где расположены компоненты автоматизированных систем);

• сотрудники службы безопасности автоматизированных систем;

• руководители различных уровней должностной иерархии.

Посторонние лица, которые могут быть нарушителями:

• клиенты (представители организаций, граждане);

• посетители (приглашенные по какому-либо поводу);

• представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации (энерго-, водо-, теплоснабжения и т.п.);

• представители конкурирующих организаций (иностранных спецслужб) или лица, действующие по их заданию;

• лица, случайно или умышленно нарушившие пропускной режим (без цели нарушить безопасность автоматизированных систем);

• любые лица за пределами контролируемой территории.

Причиной совершения компьютерных преступлений может быть:

- личная или финансовая выгода;

- развлечение;

- месть;

- попытка добиться расположения кого-либо к себе;

- самовыражение;

- случайность;

- вандализм.

Можно выделить три основных мотива нарушений: безответственность, самоутверждение и корыстный интерес.

При нарушениях, вызванных безответственностью, пользователь целенаправленно или случайно производит какие-либо разрушающие действия, не связанные тем не менее со злым умыслом. В большинстве случаев это следствие некомпетентности или небрежности.

Нарушение безопасности АС может быть вызвано и корыстным интересом пользователя системы. В этом случае он будет целенаправленно пытаться преодолеть систему защиты для доступа к хранимой, передаваемой и обрабатываемой в автоматизированных системах информации. Даже если автоматизированная система имеет средства, делающие такое проникновение чрезвычайно сложным, полностью защитить ее от проникновения практически невозможно.

Всех нарушителей можно классифицировать следующим образом:

- По уровню знаний об автоматизированных системах

- По уровню возможностей (используемым методам и средствам)

- По времени действия

- По месту действия

Определение конкретных значений характеристик возможных нарушителей в значительной степени субъективно. Модель нарушителя, построенная с учетом особенностей конкретной предметной области и технологии обработки информации, может быть представлена перечислением нескольких вариантов его облика. Каждый вид нарушителя должен быть охарактеризован значениями характеристик, приведенных выше.

Возможный ущерб автоматизированной системе и обрабатываемой информации зависит от уровня возможностей нарушителя (злоумышленника), который может обладать правами: разработчика, программиста, пользователя, администратора.

Результатом реализации угроз информации может быть ее утрата (разрушение, уничтожение),утечка (извлечение, копирование), искажение (модификация,

подделка) или блокирование.

По степени преднамеренности проявления различают случайные и преднамеренные угрозы безопасности.

По непосредственному источнику угроз. Источниками угроз могут быть:

- природная среда, например, стихийные бедствия;

- человек, например, разглашение конфиденциальных данных;

- санкционированные программно-аппаратные средства, например, отказ в работе операционной системы;

- несанкционированные программно-аппаратные средства, например, заражение компьютера вирусами.

По положению источника угроз. Источник угроз может быть расположен:

- вне контролируемой зоны КС, например, перехват данных, передаваемых по каналам связи;

- в пределах контролируемой зоны КС, например, хищение распечаток, носителей информации;

- непосредственно в КС, например, некорректное использование ресурсов.

По степени воздействия на КС различают:

- пассивные угрозы, которые при реализации ничего не меняют в структуре и содержании КС (угроза копирования данных);

- активные угрозы, которые при воздействии вносят изменения в структуру и содержание КС (внедрение аппаратных и программных спецвложений).

По этапам доступа пользователей или программ к ресурсам КС:

- угрозы, которые могут проявляться на этапе доступа к ресурсам КС;

- угрозы, проявляющиеся после разрешения доступа (несанкционированное использование ресурсов).

По текущему месту расположения информации в КС:

- угроза доступа к информации на внешних запоминающих устройствах (ЗУ), например, копирование данных с жесткого диска;

- угроза доступа к информации в оперативной памяти (несанкционированное обращение к памяти);

- угроза доступа к информации, циркулирующей в линиях связи (путем незаконного подключения).

По способу доступа к ресурсам КС:

- угрозы, использующие прямой стандартный путь доступа к ресурсам с помощью незаконно полученных паролей или путем несанкционированного использования терминалов законных пользователей;

- угрозы, использующие скрытый нестандартный путь доступа к ресурсам КС в обход существующих средств защиты.

По степени зависимости от активности КС различают:

- угрозы, проявляющиеся независимо от активности КС (хищение носителей информации);

- угрозы, проявляющиеся только в процессе обработки данных (распространение вирусов).

Человека, пытающегося нарушить работу информационной системы или получить несанкционированный доступ к информации, обычно называют взломщиком, а иногда «компьютерным пиратом».

Противоправные действия с информацией не только затрагивают интересы государства, общества и личности, но оказывают негативные, а порой трагические и катастрофические воздействия на здания, помещения, личную безопасность обслуживающего персонала и пользователей информации. Подобные воздействия происходят также по причине стихийных бедствий, техногенных катастроф и террористических актов.

Главной целью любой системы обеспечения информационной безопасности является создание условий функционирования предприятия, предотвращение угроз его безопасности, защита законных интересов предприятия от противоправных посягательств, недопущение хищения финансовых средств,

разглашения, утраты, утечки, искажения и уничтожения служебной информации, обеспечение в рамках производственной деятельности всех подразделений предприятия.

Заключение

Возможные последствия IT-угроз:

- Финансовые потери
- Потеря конкурентного преимущества
- Потеря доли рынка
- Штрафные санкции регуляторов
- Угроза стабильности работы инфраструктур
- Потеря клиентов и партнеров
- Ущерб репутации предприятий и их главных лиц

Далее приведем некоторые жизненные примеры атак и утечек, а также как результат их масштабы:

Рисунок 7. Ежегодный рост утечки информации

Пример 1. Утечка информации

«Синдром Клинтон», сентябрь 2016

Хиллари Клинтон было не всегда удобно вести переписку, используя рабочую почту, поэтому она пересылала письма, содержащие конфиденциальную информацию, по внешней почте.

Кроме того, опасаясь хранить важную переписку у себя, она организовала хранение рабочих писем Госдепартамента США на личном сервере.

В итоге эти действия привели к утечке информации, составляющей гостайну.

Результат: скандал, подрыв репутации, выборы проиграны.

Пример 2. Целевая атака

Атака на ЦБ Бангладеш, февраль 2016

Используя социальную инженерию и рассылку писем с вирусом, хакеры проникли в систему ЦБ Бангладеш.

Злоумышленники получили доступ к межбанковской электронной системе передачи информации и совершения платежей SWIFT и попытались направить 35 мошеннических платежных поручений на общую сумму 951 млн долларов.

Хакерам удалось успешно осуществить четыре транзакции и перевести украденные деньги на Филиппины и Шри-Ланку.

Результат: убытки составили $81 млн

Пример 3. DDoS-Атака

Серия DDoS-атак на банки, ноябрь 2016

10 ноября ЦБ РФ заявил, что 5 российских банков подверглись хакерской атаке. Под ударом оказались Сбербанк, Альфа-банк, «Открытие», «ВТБ Банк Москвы» и Росбанк.

По оценке специалистов мощность атак варьировалась от «слабой» до «мощной». Длительность атак составляла от 1 до 12 часов. Некоторые банки подверглись серии от 2 до 4 атак.

Хакеры, организовавшие атаку, использовали ботнет (сеть зараженных устройств), в которую входило 24 000 машин из «Интернета вещей».

Издание Vice сообщило, что за атакой могут стоять «люди, недовольные возможным вмешательством России в выборы президента США». Российские специалисты считают, что атака – это лишь «демонстрация возможностей», а ее причины – сугубо экономические.

Результат: 3 из 5 банков подтвердили атаку

Пример 4. Ботнет «MIRAI»

В конце 2016 года произошла мощная DDoS-атака против Dyn DNS, оператора DNS в США. Атака была реализована при помощи ботнета Mirai, первого вируса для «Интернета вещей». Сотни тысяч камер, серверов DVR и других подключенных устройств вплоть до кофеварок с Wi-Fi стали оружием в руках хакеров.

Результат: Одни из самых посещаемых веб-сайтов в мире часами были недоступны для пользователей, а именно: Twitter, Spotify, Reddit, GitHub, сайты CNN, The New York Times и др.

Пример 5. Информационная атака

Атака на Сбербанк, 18.12.2014

Предпосылка: Пиковый рост курса валют Суть атаки: Активность около 80–300 аккаунтов в сети на тему (большинство – украинские):

- «Visa прекращает операции по картам Сбербанка» - «Сбербанк скоро прекратит выдачу депозитов» - «Нельзя снять деньги в банкомате, это не технический сбой – денег нет»

Граждане бросились забирать деньги. ЦБ и Правительство предприняли беспрецедентные меры по урегулированию ситуации.

Результат: Общий отток денежных средств с депозитов и из банкоматов составил примерно 1,5 трлн руб., которые были довольно быстро восстановлены.

Как видно из примеров угрозы и утечки имеют достаточно серьёзные последствия.

Как защищаться от внутренних угроз и утечек информации?

а) Для персонала – соблюдение правил обращения с информацией:

- Не использовать публичные почты для пересылки конфиденциальной информации

- Не оставлять ноутбуки, смартфоны без присмотра

- Не разглашать информацию в социальных сетях

- Помнить о шпионских функциях смартфонов

b) Для организации:

- Выявление наиболее вероятных угроз со стороны сотрудников
- Положение о коммерческой тайне и защите персональных данных
- Выбор и назначение ответственных за безопасность
- Разработка процедур по защите информации

Использование технических средств защиты от утечек Data Loss Prevention, программный комплекс, осуществляющий анализ потоков данных, пересекающих периметр защищаемой локальной сети. При обнаружении в этом потоке данных конфиденциальной информации срабатывает активная компонента системы, которая оповещает ответственного специалиста и, при необходимости, блокирует передачу данных либо решения других производителей.

Перечень мер информационной безопасности:

Использование паролей:
- Не используйте один пароль для всех сервисов, которыми вы пользуетесь. Рекомендуется использовать разные пароли для разных сервисов
- Используйте пароли длиной не менее 8 символов с содержанием строчных и прописных букв, а также цифр и спецсимволов (@, &, % и т.д.). Альтернативной хорошей практикой является использование парольных фраз, состоящих из не менее чем 20 символов, например, «ForestWinterSnowstorm» – их легко запомнить и трудно подобрать
- Не сохраняйте пароли в веб-браузерах и клиентах электронной почты
- Не передавайте пароли знакомым и не отправляйте по электронной почте
- Тщательно храните пароли. Нельзя оставлять записанный пароль на видном месте, клеить его на монитор и т.д.

Защита рабочих станций и собственных устройств:
- Все файлы, скачанные из сети Интернет, перед открытием проверяйте антивирусной программой
- При получении по электронной почте писем от неизвестных вам лиц, содержащих ссылки и картинки, рекомендуется сразу удалять, не переходя по ссылкам и не открывая приложенные документы
- Пользуйтесь лицензионным антивирусным ПО, настройте автоматическую проверку загруженных из сети файлов и подключенных носителей информации
- При возникновении признаков появления вирусов на компьютере проведите

полную проверку антивирусным ПО
- Всегда устанавливайте последние обновления операционных систем
- Для защиты от вирусов шифровальщиков регулярно создавайте резервные копии ценных для вас данных

Безопасность при осуществлении платежей:
- По возможности, следует использовать дополнительное подтверждение операций, например, с помощью SMS или иным способом (например, по телефону)
- Не переходите по ссылкам, полученным от недоверенных лиц. При получении писем или сообщений от банков удостоверьтесь, что это именно банк пишет вам
- Будьте внимательны при осуществлении платежей в сети Интернет. Проверяйте наличие https в адресной строке браузера и точность адреса

Использование сети Интернет и социальных сетей:
- Не пользуйтесь незащищенными Wi-Fi-сетями
- С осторожностью относитесь к нестандартным сообщениям в сети Интернет (особенно в социальных сетях). Помните, что любые нестандартные просьбы могут быть мошенничеством
- Не используйте бесплатную почту и чаты для передачи критически важной информации

Защита важной информации:
- Используйте шифрование при передаче критически важной информации
- С осторожностью относитесь к хранению информации в облаке. Следует шифровать данные для хранения их в облаке либо сделать выбор в пользу хранения информации локально
- Не берите смартфон на важные переговоры
- Не используйте мобильное устройство для конфиденциальной переписки

Список использованной литературы

1. Макаренко С. И. Информационная безопасность: учебное пособие для студентов вузов. – Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. – 372 с.: ил., Часть 1, раздел 4

2. Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. - М.: Академический Проект; Гаудеамус, 2-е изд.- 2004. - 544 с., параграфы 2.3, 5.1-5.5

3. Денисов Д.В. Информационная безопасность: Интернет курс

4. Кияев В.И., Граничин О.Н. Безопасность информационных систем

5. О безопасности: Федер. закон [принят Гос. Думой 07.12.2010 (ред. от 05.10.2015)] // N 390-ФЗ.