Содержание:

ВВЕДЕНИЕ

Все по большей части в былое уходит излишнее нагромождение разнообразных средств защиты, которое стало «модным» в итоге реакции на первую волну страха перед компьютерными правонарушениями. К тому, что защита информации должна быть носить комплексной, все начинают понемногу свыкаться. При этом компании - заказчики по большей части не собираются выкидывать деньги на ветер, они собираются покупать только то, что им вправду нужно для создания надежной системы по защите информации. Но организация, которая обеспечивает безопасность информации обязана не только носить комплексной, но еще строиться на глубоком анализе вероятных отрицательных последствий. При этом всем значимо не пропустить какие-либо важнейшие аспекты.

Процесс значимости в России международных стандартов по защите информации не является изолированным исключительным решением, а делается естественной составной частью реформирования целой системы стандартизации. сегодня в России наравне с отечественной нормативной базой обширно применяются около 140 международных стандартов в сфере информационных технологий, из них примерно 30 касаются вопросов по защите информации.

Одним из наиболее существенных является стандарт ИСО/МЭК 15408–99. «Критерии оценки безопасности информационных технологий», более известный как «Общие критерии». Этот стандарт привносит новую методологию создания запросов по безопасности информационных технологий, соответствующих современному уровню их развития, и методологию оценки безопасности продуктов и систем информационных технологий.

Но вся идеология этого стандарта выстроена на необходимости глубокого исследования и анализа имеющейся обстановки и, особенно, раскрытии актуальных угроз информационной безопасности. При этом должны быть оценены все угрозы, с которыми можно столкнуться, и избраны только те, которые могут воздействовать на безопасность информации. Стандарт предполагает, что при обрисовке угроз обязательно должен быть идентифицирован источник этих угроз, метод воздействия, уязвимости, свойственные объекту и многое остальное.

Собственно поэтому выбор верной методологии оценки вероятных угроз информационной безопасности является одним из существенных направлений при переходе к международным требованиям.
Целью курсовой работы является рассмотрение угроз информационной безопасности и способов их реализации, анализ критериев уязвимости и устойчивости систем к деструктивным воздействиям**.**

1. ВИДЫ И СОСТАВ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Под угрозой безопасности информации осмысливается совокупность обстоятельств и факторов, организовывающих возможную или реально имеющуюся опасность нарушения безопасности информации.

Фактор, влияющий на защищаемую информацию - это действие, явление или процесс, итогом которого могут быть утечка, коверкание, уничтожение защищаемой информации и блокирование доступа к ней.

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

Уязвимость информационной системы - свойство информационной системы, определяющее вероятность осуществления 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 (рис. 1.1).Как правило, вышеперечисленные угрозы информационным ресурсам осуществятся следующими способами: Через имеющиеся агентурные источники в органах государственного управления и коммерческих структурах, обладающих возможностью получения секретной информации (суды, налоговые органы, коммерческие банки). Путем подкупа лиц, прямиком трудящихся в организации или структурах, напрямую связанных с ее занятием.

1. Путем перехвата информации, циркулирующей в средствах и системах связи и вычислительной технике при помощи технических приборов разведки и съема

информации.

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

Угрозы информационной

безопасности

Проявляются в нарушениях

ЦЕЛОСТНОСТИ

КОНФИДЕНЦИАЛЬНОСТИ

ДОСТУПНОСТИ

Разглашение

Утечка

НДС

Искажения

Ошибки

Потери

Фальсификации

Нарушение связи

Воспрещение получения

Рис. 1 Влияние угроз информации на критерии информационной безопасности

Информационная безопасность оказывает воздействие на защищенность интересов в всевозможных сферах жизнедеятельности общества и государства. В каждой из них есть свои особенности обеспечения информационной безопасности, связанные со спецификой предметов обеспечения безопасности, уровнем их уязвимости в отношении угроз информационной безопасности.

Например, с точки зрения обеспечения безопасности информации в компьютерных системах большое количество потенциальных угроз безопасности информации

можно выделить два класса.

Угрозы, которые не связаны с предумышленными действиями злоумышленников и осуществятся в случайные моменты времени, именуют случайными или непреднамеренными.

Осуществление угроз этого класса повергает к самым большим потерям информации. При всем этом могут совершаться нарушение целостности, уничтожение и доступности информации. Редко нарушается конфиденциальность информации, но при этом формируются предпосылки для злоумышленного влияния на информацию.

Стихийные бедствия и аварии чреваты наиболее разрушительными результатами для информации, так как носители подвергаются физическому разрушению, информация теряется или доступ к ней делается невозможным.

Сбои и отказы сложных систем неизбежны. Вследствие сбоев и отказов нарушается работоспособность технических средств, теряются и искажаются данные и программы, нарушается алгоритм работы устройств. Нарушения алгоритмов работы некоторых узлов и устройств могут также повергнуть к нарушению конфиденциальности информации. Например, сбои и отказы средств отпуска информации могут привести к несанкционированному доступу к информации путем несанкционированной ее .трансляции в канал связи, на печатающее устройство и т. п.

Ошибки при разработке компьютерных систем, алгоритмические и программные ошибки приводят к последствиям, аналогичным последствиям (сбоев и отказов технических средств). Кроме того, такие ошибки могут быть применяться злоумышленниками для воздействия на ресурсы компьютерных систем. Особенную опасность представляют ошибки в операционных системах и в программных средствах защиты информации.

Другой класс угроз безопасности информации в компьютерных системах составляют умышленно формируемые угрозы. Угрозы этого класса в соответствии с их физической сути и механизмом реализации могут быть поделены на пять групп:

- традиционный или универсальный шпионаж и диверсии;
- модификация структур;
- несанкционированный доступ к информации;
- модификация структур;

- электромагнитные излучения и наводки;
- вредоносные программы.

В качестве источников нежелательного влияния на информационные ресурсы по-прежнему актуальны методы и средства шпионажа и диверсий, которые применялись и применялись для добывания или уничтожения информации. Эти методы также действенны и эффективны в условиях использования компьютерных систем. Чаще всего они используются для приобретения информации о системе защиты с целью проникнуть в систему, а также для кражи и уничтожения информационных ресурсов.

Угрозы в коммерческой деятельности также имеют свои особенности.

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

Криминальные группы и формирования.

1. Недобросовестные конкуренты.

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

3. Нарушение установленного регламента сбора, обработки и передачи информации.

Основные виды внутренних угроз:

1. Преднамеренные криминальные действия своего персонала организации.

2. Случайные действия и ошибки сотрудников.

3. Отказ оборудования и технических средств.

Сбои в программном обеспечении средств обрабатывания

информации.

Объектами всевозможных угроз в коммерческой деятельности являются:

1. Человеческие ресурсы (персонал, сотрудники, компаньоны и др.), включая трудовые и кадровые ресурсы.

2. Финансовые ресурсы.

3. Временные ресурсы.

4. Материальные ресурсы.

Информационные ресурсы, охватывая интеллектуальные ресурсы (патенты, незавершенные проектно-конструкторские разработки, ноу-хау, программные продукты, массивы бухгалтерской и статистической информации и пр.).

Наиболее серьезным ключом угроз предприятиям являются собственные сотрудники. Мотивами внутренних угроз в таких случаях является безответственность, некомпетентность (низкая квалификация), личные побуждения (самоутверждение, корыстные интересы).

В условиях сохраняющейся значительной степени монополизации российской экономики опасность предпринимательству представляет недобросовестная конкуренция, представляющая собой:

1. Все действия, ведущие к тому, что потребитель может принять предприятие, товары, промышленную или коммерческую деятельность данной организации за предприятие, товары, промышленную или коммерческую деятельность конкурента.
2. Неверные заявления в ходе коммерческой деятельности, дискредитирующие предприятие, товары, промышленную или коммерческую деятельность конкурента.
3. Употребление в ходе коммерческой деятельности указаний или обозначений, которые вводят потребителя в заблуждение относительно природы, метода изготовления, характеристик, пригодности для установленных целей или численности товаров.

Осуществление угроз в данном случае понижает эффективность и надежность функционирования организаций, а в некоторых случаях, приводят к прекращению их деятельности из-за опасности экономического, социального, правового, организационного, информационного, экологического, технического и криминального характера. Предметами угроз могут быть элементы материального, личного («человеческого»), финансового, информационного и другого капитала, составляющего экономическую основу занятия предпринимательства.

Любая угроза влечет за собой предопределенный ущерб (потери) — моральные или материальные, а меры по противодействию данной угрозы призваны уменьшить ее уровень до приемлемого уровня.

Оценка вероятных ущербов (потерь) предполагает знание видов потерь, обусловленных с предпринимательской деятельностью, и умение вычисления их вероятностной прогнозной величины. Имеются следующие виды вероятных ущербов (потерь):

1. Материальные виды потерь выражаются в непредусмотренных предпринимательским проектом лишних затратах или прямых утратах оборудования, имущества, продукции, сырья, энергии и т. д.

2. Трудовые потери — это потери рабочего времени, вызванные случайными, непредвиденными ситуациями; измеряются в часах рабочего времени. Перевод трудовых потерь в денежную формулировку реализовывается путем умножения труд часов на стоимость (цену) одного часа.

3. Кадровые потери — это потери нужных предприятию профессиональных, высококвалифицированных рабочих; измеряются в затратах на подбор и обучение новоиспеченного кадрового резерва в денежном выражении.

1. Финансовые потери — прямой денежный ущерб, связанный с непредусмотренными уплатами, уплатой дополнительных налогов, выплатой штрафов, утратой денежных средств и ценных бумаг.
2. Временные потери. Происходят, когда процесс предпринимательской деятельности идет медленнее, чем запланировано. Прямая оценка таких потерь сбывается в часах, днях, неделях, месяцах запаздывания в получении намеченного результата. Чтобы перевести оценку потерь времени в денежное измерение, надо установить, к каким потерям дохода, прибыли способны приводить потери времени. В конечном результате оцениваются в денежном выражении.
3. Информационные потери. Одни из самых обстоятельных потерь в бизнесе, способные привести к краху всей организации. Исчисляются в стоимостном выражении.
4. Особые виды потерь выражаются в виде нанесения ущерба здоровью и жизни людей, окружающей среде, авторитету предпринимателя, а также в результате других неблагоприятных социальных и морально - психологических следствий.

Информационный ущерб (потери) связан с наличием в процессе предпринимательской деятельности информационного риска, который входит в общий предпринимательский риск.

Информационный риск - вероятность (угроза) потерь активов субъекта экономики (предпринимателя) вследствие потерь, порчи, коверкания и разглашения информации.

Информационный риск группируется следующим образом:

- риск прерывания информации (прекращение нормальной обработки информации, например, в результате разрушения, вывода из строя вычислительных средств). Подобная категория действий может породить весьма серьезные последствия, если даже информация при всем этом не подвергается никаким воздействиям;
- риск кражи информации (считывание или копирование информации, хищение магнитных носителей информации и следствий печати с целью приобретения данных, которые потом могут быть употребляться против интересов владельца (собственника) информации);
- риск видоизменение информации (внесение несанкционированных изменений в данные, направленных на нанесение ущерба владельцу (собственнику) информации);

риск разрушения данных (необратимое изменение информации, повергающее к невозможности ее использования);

- риск электромагнитного влияния и перехвата информации в автоматизированных и информационных системах (АИС);
- риск съема информации по звуковому каналу;
- риск прекращения питания АИС и поддерживающей инфраструктуры);
- риск ошибки операторов и поставщиков информационных ресурсов АИС;
- риск сбоев программного обеспечения АИС;
- риск неисправности аппаратных устройств АИС (в результате небрежных действий сотрудников, несоблюдения техники безопасности, природных катаклизмов, сбоев программных средств и т. д.).

В исходном итоге все незаконные воздействия приводят к нарушению конфиденциальности, достоверности, целостности и открытости информации.

Таким образом, перечень угроз и источников их возникновения достаточно разнообразен и предложенная классификация не является исчерпывающей. Противодействие проявлениям угроз реализовывается по всевозможным направлениям, с применением совершенного арсенала методов и средств защиты.

2. ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Техническая защита информации – это защита информации, включающаяся в обеспечении не криптографическими методами безопасности информации (данных), подлежащих защите в соответствии с функционирующим законодательством, с использованием технических, программных и программно-технических средств.

Техника защиты информации - средства защиты информации, в этом числе средства физической защиты информации, криптографические средства защиты информации, средства контроля результативности защиты информации, средства и системы управления, назначенные для обеспечения защиты информации.

2.1 Технические средства защиты информации

К техническим средствам защиты информации относятся технические устройства, которые должны пресекать разглашения информации, и обеспечить защиту от утечки, и противодействия несанкционированному доступу к источникам конфиденциальной информации.

Технические средства защиты информации используются для решения следующих задач:

- обнаружение каналов утечки информации на различных объектах и в помещениях;
- проведение особых обследований технических средств обеспечения производственной деятельности на присутствие вероятных каналов утечки информации;
- устранение каналов утечки информации;
- поиск и раскрытие средств промышленного шпионажа;
- противодействие несанкционированному доступу к источникам конфиденциальной информации и прочим действиям.

По функциональному направлению технические средства защиты могут быть сгруппированы на средства поиска, детальных измерений средства выявления и средства активного и пассивного противодействия.

По своим техническим характеристикам средства защиты информации могут быть совместного назначения, рассчитанные на применение непрофессионалами с целью приобретения предварительных (общих) оценок, и профессиональные комплексы, дающие возможность проводить скрупулезный поиск, обнаружение и прецизионные измерения всех характеристик средств промышленного шпионажа.

На примере первых можно разобрать группу индикаторов электромагнитных излучений типа ИП, располагающих широким спектром обретаемых сигналов и довольно небольшой чувствительностью. В качестве второго примера - комплекс для выявления радио закладных устройств, предназначенный для автоматического обнаружения и определения месторасположения радиопередатчиков, радиомикрофонов, телефонных закладок и сетевых радиопередатчиков.

Поисковую аппаратуру можно разделить на аппаратуру поиска средств съема информации и обследования каналов ее утечки.

Аппаратура относящихся к первому типу направленных на поиск и локализацию уже внедренных злоумышленниками средств несанкционированного доступа. Аппаратура второго типа предназначается для обнаружения каналов утечки информации.

Обработка итогов измерений осуществляется на ПЭВМ в соответствии с функционирующими нормативно - методическими документами ФСТЭК России.

2.2 Программные средства защиты информации

Программная защита информации — это система специализированных программ, реализующих функции защиты информации. Отличаются следующие направления применения программ для обеспечения безопасности секретной информации

- защита информации и программ от копирования;
- защита информации и программ от разрушения и модификации;
- защита информации от несанкционированного доступа;
- программная защита каналов связи.

Защита информации от несанкционированного доступа

Для защиты от постороннего вторжения обязательно предусматриваются определенные пределы безопасности. Важнейшие функции, которые должны реализовываться программными средствами, это:

- разграничить доступа к вычислительным ресурсам и информации;
- идентификация субъектов и объектов;
- проверка и регистрация действий с информацией и программами.

Процедура идентификации и подтверждения подлинности предполагает проверку, является ли субъект, выполняющий доступ, тем, за кого себя выдает. Наиболее распространенным методом идентификации является парольная идентификация.

После выполнения операции идентификации и установления подлинности пользователь приобретает доступ к вычислительной системе, и защита информации реализовывается на трех уровнях: аппаратуры, программного обеспечения и данных.

Средства защиты от копирования предотвращают применение нелегальных копий программного обеспечения и являются едва ли единственным средством, защищающим авторское право разработчиков. Под средствами защиты от копирования осмысливаются средства, обеспечивающие выполнение программой своих функций только при индикации некоторого уникального не копируемого элемента. Таким элементом (ключевым) может быть установленная часть компьютера или специальное устройство.

Одной из задач обеспечения безопасности для всех случаев пользования компьютером является защита информации от разрушения и модификации. Так как основания разрушения информации очень разнообразны (несанкционированные действия, ошибки программ и оборудования, компьютерные вирусы и пр.), то проведение защитных мероприятий обязательно для всех, кто использует компьютером.

По любому из выше указанных назначений существует довольно большое количество сертифицированных и реализуемых на рынках программных продуктов, которые могут быть применены для защиты информации на предприятии.

Кроме того, программные средства защиты располагают следующими разновидностями специальных программ:

- идентификации технических средств, файлов и аутентификации пользователей;
- регистрации и проверки работы технических средств и пользователей;
- обслуживания режимов, обработки информации узкого круга пользователей,
- защиты операционных средств ЭВМ и прикладных программ пользователей;
- уничтожения информации в защитные устройства после применения;
- сигнализирующих нарушения применения ресурсов;
- вспомогательных программ защиты разнообразного назначения.

2.3 Программно-технические средства защиты информации

Программно-технические средства защиты информации, устремлены на контроль оборудования, программ и/или данных. Основным для программно-технического уровня является понятие сервиса безопасности. В число таких сервисов укладываются:

- идентификация и аутентификация;
- управление доступом;
- протоколирование и аудит;
- проверка целостности;
- экранирование;
- анализ защищенности;
- обеспечение отказоустойчивости;
- обеспечение безопасного восстановления;
- туннелированные;
- управление.

Эти сервисы должны работать в открытой сетевой среде с разнохарактерными компонентами, то есть быть устойчивыми к соответствующим угрозам, а их использование должно быть удобным для администраторов и пользователей.

К программно-техническим средствам защиты информации относятся:

Программно-технические средства защиты информации от несанкционированного копирования, в том числе:

- средства защиты носителей данных;

- средства предупреждения копирования программного обеспечения, установленного на ПЭВМ.

Программно-технические средства криптографической и стеганографической защиты информации (включая средства маскирования информации) при ее сохранении на носителях данных и при трансляции по каналам связи.

Программно-технические средства прерывания работы программы пользователя при нарушении им правил доступа, в том числе:

- принудительное окончание работы программы;
- блокировка компьютера.

Программно-технические средства стирания данных, в том числе:

- стирание остаточной информации, появляющейся в процессе обрабатывания данных в оперативной памяти и на магнитных носителях;
- надежное стирание отжившей свое информации с магнитных носителей.

Программно-технические средства подачи сигнала тревоги при попытке несанкционированного доступа к информации, в том числе:

- средства регистрации неучтивых обращений пользователей к защищаемой информации;
- средства организации контроля за действиями пользователей ПЭВМ.

Программно-технические средства обнаружения и локализации воздействия программных и программно-технических закладок.

3. ОРГАНИЗАЦИОННАЯ ЗАЩИТА ИНФОРМАЦИИ

3.1 Организационные мероприятия по защите информации

Организационная защита информации – это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно – правовой основе, исключающей или значительно затрудняющей неправомерное овладение конфиденциальной информацией и проявление внутренних и внешних угроз.

Основные направления организационной защиты информации представлены на рис. 2.

Организационная защита информации

Охрана

и режим

Комплексное управление системой защиты

Работа

с документами

Работа

с персоналом

Анализ внутренних и внешних угроз

Рис. 2 Направления организационной защиты информации

Организация охраны и режима имеется в виду комплекс мероприятий по исключению вероятности тайного проникновения на территорию и в помещение чужих лиц, организация отдельных охраняемых зон, временного и пропускного режима и организации контроля за персоналом и посетителями,

Организация работы с кадрами подразумевает подбор и расстановку сотрудников на штатные должности, проведение исследования морально – деловых качеств, обучение их правилам работы с секретной информацией, доведение мер ответственности, контроль за работой персонала.

Работа с документами – имеется в виду организацию разработки и применения носителей информации, их учета, использование, хранения и уничтожения.

Анализ внутренних и внешних угроз подразумевает обнаружение, классификация и непрерывное изучение ситуаций, содействующих формированию каналов несанкционированного доступа к конфиденциальной информации в единстве с изучением характера возможных угроз безопасности информации.

Комплексное управление системой защиты подразумевает наилучшее планирование использования всего комплекса средств защиты информации, технических и физических средств, организацию их эксплуатации и обслуживания.

Сложность обеспечения защиты информации требует формирования специальной службы, выполняющей реализацию всех защитных мероприятий и в первую очередь организационного плана.

3.2 Организация охраны и режима

Под организацией охраны территории предприятия (объекта) осмысливается комплекс мероприятий, сосредоточенный на пресечение несанкционированного проникновения, на контролируемую территорию (объект) сторонних лиц, а также недопущение несанкционированного выхода за пределы контролируемой территории и выноса материальных и иных средств.

Обеспечение надежной охраны объекта и режимных мероприятий позволяет исключить предпосылки несанкционированного доступа, модификации видоизменения, кражи информационных ресурсов.

В законе о частной детективной и охранной деятельности к видам охранной деятельности относятся:

1) защита жизни и здоровья граждан;

2) охрана имущества собственников, в том числе при его перевозке;

3) проектирование, монтаж и эксплуатационное обслуживание средств охранно-пожарной сигнализации;

4) консультирование и подготовка советы клиентам по вопросам правомерной защиты от противоправных посягательств;

5) обеспечение порядка в местах проведения массовых мероприятий.

Границы пространства, защищаемого от угрозы, именуют рубежами защиты. Район пространства внутри сомкнутого рубежа защиты принято называть зоной безопасности.

3.3 Организация работы с персоналом в системе информационной безопасности

Работники предприятия или персонал является одним из вероятно возможных источников утечки конфиденциальной информации и как результат финансовых потерь предприятия. Как правило, персонал содержит сведения о:

- всех без исключения работниках данного предприятия, его персонале;
- работников других организаций, фирм - посредников, изготовителей комплектующих деталей, торговых фирм, рекламных агентств и т. п.;
- сотрудников государственных учреждений, к которым организация обращается в соответствии с законом, — налоговых, муниципальных правоохранительных органов и т. д.;

Перечисленные выше лица в той или иной мере являются или могут стать в силу ситуаций источниками конфиденциальных сведений. Но наиболее информированы о конфиденциальной информации: первый руководитель, его заместитель, их референты и секретари, работающие с конфиденциальной документацией.

3.4 Организация конфиденциального делопроизводства

При работе с документами, включающие конфиденциальную информацию, необходимо соблюдать установленные правила. Это дает гарантии надежной охраны коммерческих информационных ресурсов и устанавливает заслон на дороге к утечкам информации. Эти правила сводятся к следующему:

- жесткий контроль (лично или через службу безопасности) за допуском персонала к конфиденциальным документам;
- определение конкретных лиц из руководства и служащих, которые организуют и контролируют делопроизводство, и наделение их должными полномочиями;
- разработка должностных инструкции (памятки) по работе с конфиденциальными документами, донесение их соответствующим работникам;

- контроль о принятием соответствующими служащими письменных обязательств о хранении коммерческой тайны;
- введение системы материального и иного стимулирования служащих, обладающих правом доступа к конфиденциальной информации;
- внедрение в обыденную практику механизмов и технологий защиты коммерческой тайны;
- персональный контроль со стороны начальника, службы безопасности конфиденциального делопроизводства.

Для ведения конфиденциального делопроизводства должны привлекаться сотрудники, прошедшие особую проверку, и надлежащим образом подготовленные и обученные.

Помещения, в которых ведутся работы с конфиденциальными документами, должны хорошо охраняться, а вход посторонним должен быть закрыт. Эти помещения должны быть оборудованы прочными перекрытия и стенами, иметь усиленную металлическую дверь. Оконные рамы должны быть с двойными стеклами и решеткой, повешены плотные шторы или жалюзи. Хранилище следует оборудовать охранной и пожарной сигнализацией и скрупулезно охраняться силами внутренней охраны. Доступ в хранилище железно ограничен. Не рекомендуется иметь такое помещение на первом и последнем этажах здания. Конфиденциальные документы должны хранится в сейфах или несгораемых металлических шкафах с надежными замками и запорами.

3.5. Аналитическая работа по выявлению каналов утраты информации

В основе отыскивания и выявления каналов утраты конфиденциальной информации лежит непрерывная аналитическая работа - обнаружение, классификация и постоянное изучение ситуаций, содействующих организации каналов несанкционированного доступа к конфиденциальной информации в единстве с исследованием характера допустимых угроз безопасности информации.

Эта работа имеет предупредительный и информационный характер о состоянии внутренней и внешней, сфер деятельности предприятия, т. е. сосредоточена на исследование комплекса вероятных угроз. Другие пути носят случайный характер ожидания ошибки в поступках злоумышленника, т. к. истинные каналы

разглашения или утечки конфиденциальной информации всегда являются секретом злоумышленника.

Результаты аналитической работы представляют собой степень защищенности интеллектуальной собственности и условий функционирования предприятия. Они являются основой для разработки и систематического совершенствования комплекса защиты информации, определения ее структуры и цены в соответствии с подлинными опасностями, угрожающими ценным информационным ресурсам. Аналитическое исследование дает возможность разработать способы пассивного и активного противодействия злоумышленнику в организационных и технических каналах.

Направления аналитической работы по выявлению каналов несанкционированного доступа к дорогой и конфиденциальной информации в общем виде следующие:

- анализ каналов объективного распространения этой информации;
- анализ источников конфиденциальной информации;
- аналитическая работа с источником угрозы информации.

Источники угрозы могут быть внешними и внутренними. **Внешние** источники находятся вне организации и изображены чрезвычайными ситуациями, а также организационными структурами и физическими лицами, изъявляющими определенную заинтересованность к деятельности предприятия. Внутренние источники угрозы связаны с фатальными событиями в здании или помещениях предприятия, а также с персоналом. Однако наличие источника угрозы само по себе не является угрозой. Угроза реализуется в действиях.

Интересы и устремления конкурентов, вырабатывание угроз утраты конфиденциальной информации отыскиваются в основном за счет анализа публикаций, рекламных, выставочных и других материалов фирм-конкурентов, высказываний их сотрудников в печати или устных выступлениях, беседах, анализа изданных результатов финансово-хозяйственной деятельности этих фирм. Нужные итоги дает сформированная информационно-аналитическая группа.

Контрольная и аналитическая работа проводится при потенциальных и пассивных угрозах источникам информации и каналам ее распространения. В условиях активной угрозы одновременно осуществляется заблаговременно спланированное, обдуманное и решительное противодействие злоумышленнику.

Наличие, ведение и итоги постоянной аналитической работы определяют нужность, структуру и содержание системы защиты информации, требуемую степень ее результативности и направления совершенствования. При отсутствии в организации обстоятельной аналитической работы делается практически невозможным выявление и контроль каналов утраты ценной и конфиденциальной информации.

3.6 Комплексное управление системой защиты информации

Комплексное управление системой защиты информации предприятия реализовывается на основе принятой и действующей политики информационной безопасности. С практичной точки зрения политику безопасности разумно разбирать по трем уровням детализации.

К верхнему уровню можно отнести решения, затрагивающие организацию в целом. Они носят общий характер и, как правило, идут от лица руководства организации. Ориентировочный список близких решений может содержать в себя следующие элементы:

решение выработать или переделать комплексную программу обеспечения информационной безопасности, назначение ответственных за продвижение программы;

формулировка целей, которым стремится организация в области информационной безопасности, установление общих направлений в достижении этих целей;

обеспечение базы для соблюдения законов и правил;

формулировка административных постановлений по тем вопросам осуществлению программы безопасности, которая должна рассматриваться на уровне организации в целом.

Для политики верхнего уровня цели организации в области информационной безопасности выражаются в терминах целостности, доступности и конфиденциальности. Если организация несет ответственность за поддержание критически значимых баз данных, на первом плане может стоять снижение числа потерь, повреждений или искажений данных.

Для организации, торгующей компьютерной техникой немаловажна актуальность информации о предоставляемых услугах и ценах и ее доступность большому числу потенциальных покупателей.

Руководство режимного предприятия в основную заботу уделяет защите от несанкционированного доступа, то есть конфиденциальности.

На верхний уровень выносится управление защитными ресурсами и координация применения данных ресурсов, выделение особого персонала для защиты критически существенных систем и сотрудничество с другими организациями, обеспечивающими или контролирующими порядок безопасности.

Политика верхнего уровня должна четко обрисовывать круг своего влияния. В политике должны быть установлены обязанности должностных лиц по формированию программы безопасности и проведению ее в жизнь. В этом значении политика безопасности является основой подотчетности персонала.

Политика верхнего уровня располагает тремя аспектами законопослушности и исполнительской дисциплины. Во-первых, организация обязана соблюдать имеющиеся законы. Во-вторых, следует контролировать действия лиц, ответственных за выработку программы безопасности. Наконец, нужно обеспечить установленную степень исполнительности персонала, а для этого необходимо разработать систему поощрений и наказаний.

К среднему уровню можно причислить вопросы, касающиеся некоторые аспекты информационной безопасности, но существенные для различных эксплуатируемых организацией систем. Примеры таких вопросов - взгляд на прогрессивные технологи, доступа в Internet, применение домашних компьютеров, использование пользователями неофициального программного обеспечения и т.д.

Политика безопасности нижнего уровня относится к конкретным информационным сервисам. Она содержит в себе два аспекта - цели и правила их достижения. В отличие от двух верхних уровней, рассматриваемая политика должна быть определена более подробно. Примеры вопросов, на которые следует дать ответ в политике безопасности нижнего уровня:

кто имеет право доступа к объектам, поддерживаемым сервисом?

при каких ситуациях можно читать и изменять данные?

как образован удаленный доступ к сервису?

При формулировке целей политики нижнего уровня можно исходить из суждений целостности, открытости и конфиденциальности, но не разрешается на этом останавливаться. Ее цели должны быть более конкретными. Например, если речь идет о системе расчета заработной платы, можно установить цель, чтобы только лишь сотрудникам отдела кадров и бухгалтерии разрешалось вводить и изменять информацию.

В более общем случае цели должны объединять между собой объекты сервиса и воздействия с ними. Из целей формируются правила безопасности, описывающие, кто, что и при каких-либо обстоятельствах может делать. Чем детальнее правила, чем более формально они изложены, тем проще поддержать их выполнение программно-техническими средствами.

Организация деятельности предприятия по обеспечению информационной безопасности обязаны соответствовать современным международным запросам в данной области. Стандарт информационной безопасности ISO/IEC 27002 – это информационные технологии.

Технологии безопасности. Утилитарные правила менеджмента информационной безопасности (англ. Information technology — Security techniques — Code of practice for information security management). разработаны в 2005 году на основе версии ISO 17799.

Стандарт предоставляет оптимальные практические рекомендации по менеджменту информационной безопасности для тех, кто несет ответственность за разработку, реализацию или сервисное обслуживание систем менеджмента информационной безопасности. Информационная безопасность обусловливаться стандартом как сохранение конфиденциальности, целостности и доступности информации.

Нынешняя версия стандарта заключается в следующих основных разделах:

Политика безопасности (Security policy);

Организация информационной безопасности (Organization of information security);

Физическая безопасность и безопасность окружения (Physical and environmental security);

Управление ресурсами (Asset management);

Безопасность персонала (Human resources security);

Приобретение, разработка и поддержка систем (Information systems acquisition, development and maintenance);

Управление коммуникациями и операциями (Communications and operations management);

Управление доступом (Access control);

Управление бесперебойной работой организации (Business continuity management);

Управление инцидентами информационной безопасности (Information security incident management);

Соответствие нормативным требованиям.

3.7 Нормативно-методическое обеспечение защиты информации

Нормативно-методическое обеспечение защиты информации определена для регламентации процессов обеспечения безопасности информации предприятия, в этом числе и работа персонала с конфиденциальной информацией, документами, делами и базами данных.

Оно заключает в себе ряд непременных организационных, инструктивных и информационных документов, определяющих принципы, требования и способы противодействия бездейственным и активным угрозам ценной информации, которые могут возникнуть по вине персонала, конкурентов, злоумышленников и других лиц.

Нормативно-методическое обеспечение основывается на тех обязательных положениях, которые должны заключаться в учредительных и иных основных документах организации и определять правовой статус ее информационной безопасности. Указанные положения разрешают на законных основаниях вести разговор о сохранении коммерческой тайны, выделять ценную информацию, составляющую собственность организации и реализовывать действия по ее защите.

Основными организационными документами, фиксирующими задачи, функции и ответственность служб, исполняющих защиту ценной документированной информации, являются:

положение о службе безопасности,

положение о службе конфиденциальной документации,

служебные инструкции работников данных служб,

должностная инструкция менеджера (референта) по безопасности маленькой предпринимательской фирмы и др.

Технологические инструктивные документы различаются большим многообразием и по своему назначению, составу и содержанию отражают выбранную технологию системы защиты информации. Можно выделить важнейшие регламентирующие документы, располагающие значением для любого предприятия и нужные при использовании любой системы защиты информации или некоторых элементов такой системы.

Прежде всего, следует назвать Перечень конфиденциальных знаний предприятия и классифицированный список документов, подлежащих защите.

Инструкция по обеспечению безопасности конфиденциальной информации, отражающая:

режим доступа работников к конфиденциальным документам и базам данных, методом оформления документа для доступа;

обязанности сотрудников при работе с конфиденциальной информацией;

обеспечение сохранности документов на бумажных и магнитных носителях при работе с ними руководителей, исполнителей (специалистов) и технического персонала;

требования к помещениям для работы с конфиденциальной информацией;

порядок сохранения коммерческой при проведении совещаний, заседаний и переговоров;

порядок охраны территории, здания, помещений, транспортных средств и персонала;

пропускной режим в помещения, учет и распорядок выдачи удостоверений, пропусков и визуальных идентификаторов;

порядок приема, учета и контроля занятий посетителей;

запросы к защите информации в рекламной и выставочной работе, публикациях, при интервьюировании и собеседованиях;

ответственность работников за разглашение конфиденциальной информации и утрату ценных документов;

организационное обеспечение защиты информации в ПЭВМ и линиях связи, при применении в обрабатывании документов под средством оргтехники.

Инструкции по обработке, хранению и движению конфиденциальных документов определена для организации работы сотрудников службы конфиденциальной документации, менеджера (референта) по безопасности, управляющего делами, секретаря-референта первого руководителя.

Информационные документы (правила, требования, указания, методики, памятки и т. п.), детализирующие этапы по защите информации, носящие неукоснительный характер и определяющие порядок работы с конфиденциальной информацией и документами некоторых категорий работников, или всех работников в конкретных типовых ситуациях. При необходимости они могут разбираться по каждому отдельному работнику.

В порядке работы менеджера по безопасности (администратора информационной безопасности) с конфиденциальными документами и базами данных должны отображаться:

организация доступа исполнителей к конфиденциальным документам;

порядок приема и отправки конфиденциальных документов;

порядок учета (регистрации) поступающих документов;

разделение документов по руководителям и исполнителям, знакомство с документами исполнителей и передача документов на реализацию исполнения;

создание и ведение справочной - информации данных по секретным документам;

порядок организации приема руководителем посетителей, методы обеспечения безопасности руководителя;

контроль осуществления работ по документам;

ведение учета и изготовление документов на пишущих устройствах;

осуществлять формирование и хранение дел;

оформление и ведение номенклатуры дел;

защиту информации при проведении телефонных переговоров и передача информации по факсимильной связи;

защиту информации при работе с ПЭВМ;

построение систем охраны кабинета руководителя, приемной, сейфов, шкафов с документацией, вычислительной и организационной техники в рабочее и нерабочее время;

ответственность за неисполнение правил работы с конфиденциальной документацией и базами данных.

Информационные документы регламентируют запросы по единообразному выполнению персоналом установленных видов типовых действий. К этаким документам можно причислить, например, Правила обеспечения безопасности и защиты конфиденциальной информации в экстремальных ситуациях, содержащие в себе:

классифицированный перечень экстремальных ситуаций и соответствующих мероприятий по защите конфиденциальной информации, информации и документов;

порядок охраны имущества, оборудования и технических средств защиты информации;

порядок действий с правоохранительными органами при возникновении экстремальных условий.

порядок (при необходимости — план) эвакуации и охраны документов, дел и баз данных;

порядок (при необходимости — план) эвакуации и оказания содействия персоналу;

порядок охраны персонала при индивидуальных экстремальных ситуациях (угрозах, шантаже, нападении и т. п.).

ЗАКЛЮЧЕНИЕ

Информационная безопасность относится к числу направлений деятельности, формирующихся весьма резвыми темпами. Этому способствуют как всеобщий процесс развития информационных технологий, так и постоянная борьба между теми, кто желает добыть конфиденциальную информацию и теми кто хочет ее сохранить.

Опыт показывает, что для достижения результативных решений по защите информации необходимо сочетание правовых, организационных и технических мероприятий. То есть обеспечение защиты информации и в целом информационной безопасности современных информационных систем призывает применять комплексный подход. Он невозможен без использования обширного спектра защитных средств, объединенных в продуманную архитектуру.

В данных условиях позиция по отношению к защите информации обязана быть динамичной. Теоретические взгляды, стандарты, сформировавшиеся порядки надо постоянно сверять с требованиями практики. От потенциальных атак на информацию не защититься без регулярной и целенаправленной работы в данном направлении. Реальное состояние безопасности требует ежедневного участия всех заинтересованных сторон.

Список использованной литературы

1.Завгородний В.И. Комплексная защита информации в компьютерных системах: Учеб. пособие. – М.: Логос, 2001. – 264 с.

2. Домарев В.В. Безопасность информационных технологий. Системный подход – К.: ООО ТИД Диа Софт, 2014. – 992 с.
3. Кияев В., Граничин О. Безопасность информационных систем: Национальный Открытый Университет «ИНТУИТ» 2016. -192 с.

4. Минин И. В., Минин О. В.: Защита конфиденциальной информации при электронном документообороте: учебное пособие «НГТУ 2014.- 120 с.

5. Партыка Т.Л., Попов И.И. Информационная безопасность. Учебное пособие для студентов учреждений среднего профессионального образования. – М.: ФОРУМ: ИНФРА-М, 2013. – 386с.

6. Завгородний В.И. Комплексная защита информации в компьютерных системах: Учеб. пособие. – М.: Логос, 2001. – 264 с.

7. Филин С.А. Информационная безопасность. Учебное пособие. – М.:Альфа – Пресс, 20014. – 412 с.

8. Цирлов В.Л. Основы информационной безопасности: Издательство «Феникс» 20013.-256с