ГОСУДАРСТВЕННЫЙ КОМИТЕТ СВЯЗИ, ИНФОРМАТИЗАЦИИ И ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ РЕСПУБЛИКИ УЗБЕКИСТАН

ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

РЕФЕРАТ

По дисциплине: Комплексная система защиты информации

На тему: Способы защиты информации

Выполнил: Шазимов А.

Группа 233-12

Принял(а): _____

Ташкент – 2014

СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИИ

Способы - это порядок и приемы использования сил и средств для достижения поставленной цели по защите конфиденциальной информации.

1. Подальше положишь - поближе возьмешь.
2. Береженого Бог бережет.
3. На Бога надейся, а сам не плошай.
4. Сначала подумай, потом говори.
5. Не зная броду, не суйся в воду.
6. Семь раз отмерь, один раз отрежь.
7. Дело мастера боится.
8. Негоже, когда сапоги тачает пирожник, а пироги печет сапожник.
9. Отыщи всему начало, и ты многое поймешь (К. Прутков).

Любое действие человека, ориентированное на достижение каких-либо результатов, реализуется определенными способами. Естественно, что имеющийся опыт по защите информации достаточно четко определил совокупность приемов, сил и средств, ориентированных на обеспечение информационной безопасности. С учетом этого можно так определить понятие способов защиты информации: способы защиты информации - это совокупность приемов, сил и средств, обеспечивающих конфиденциальность, целостность, полноту и доступность информации, и противодействие внутренним и внешним угрозам.

Естественно предположить, что каждому виду угроз присущи свои специфические способы, силы и средства.

1.1. Общие положения

Обеспечение информационной безопасности достигается системой мер, направленных:

на предупреждение угроз. Предупреждение угроз - это превентивные меры по обеспечению информационной безопасности в интересах упреждения возможности их возникновения;

на выявление угроз. Выявление угроз выражается в систематическом анализе и контроле возможности появления реальных или потенциальных угроз и своевременных мерах по их предупреждению;

на обнаружение угроз. Обнаружение имеет целью определение реальных угроз и конкретных преступных действий;

на локализацию преступных действий и принятие мер по ликвидации угрозы или

конкретных преступных действий;

на ликвидацию последствий угроз и преступных действий и восстановление статус-кво.

Предупреждение возможных угроз и противоправных действий может быть обеспечено самыми различными мерами и средствами, начиная от создания климата глубоко осознанного отношения сотрудников к проблеме безопасности и защиты информации до создания глубокой, эшелонированной системы защиты физическими, аппаратными, программными и криптографическими средствами.

Предупреждение угроз возможно и путем получения (если хотите - и добывания) информации о готовящихся противоправных актах, планируемых хищениях, подготовительных действиях и других элементах преступных деяний. Для этих целей необходима работа сотрудников службы безопасности с информаторами в интересах наблюдения и объективной оценки ситуации как внутри коллектива сотрудников, особенно главных участков ее фирмы, так и вне, среди конкурентов и преступных формирований.

В предупреждении угроз весьма существенную роль играет информационно-аналитическая деятельность службы безопасности на основе глубокого анализа криминогенной обстановки и деятельности конкурентов и злоумышленников.

Выявление имеет целью проведение мероприятий по сбору, накоплению и аналитической обработке сведений о возможной подготовке преступных действий со стороны криминальных структур или конкурентов на рынке производства и сбыта товаров и продукции. Особое внимание в этом виде деятельности должно отводиться изучению собственных сотрудников. Среди них могут быть и недовольные, и неопытные, и "внедренные".

Обнаружение угроз - это действия по определению конкретных угроз и их источников, приносящих тот или иной вид ущерба. К таким действиям можно отнести обнаружение фактов хищения или мошенничества, а также фактов разглашения конфиденциальной информации или случаев несанкционированного доступа к источникам коммерческих секретов. В числе мероприятий по обнаружению угроз значительную роль могут сыграть не только сотрудники СБ, но и сотрудники линейных подразделений и служб фирмы, а также технические средства наблюдения и обнаружения правонарушений.

Пресечение или локализация угроз - это действия, направленные на устранение действующей угрозы и конкретных преступных действий. Например, пресечение подслушивания конфиденциальных переговоров за счет акустического канала утечки информации по вентиляционным системам.

Ликвидация последствий имеет целью восстановление состояния, предшествовавшего наступлению угрозы. Например, возврат долгов со стороны заемщиков. Это может быть и задержание преступника с украденным

имуществом, и восстановление разрушенного здания от подрыва и др.

Все эти способы имеют целью защитить информационные ресурсы от противоправных посягательств и обеспечить:

предотвращение разглашения и утечки конфиденциальной информации;
воспрещение несанкционированного доступа к источникам конфиденциальной информации; сохранение целостности, полноты и доступности информации;
соблюдение конфиденциальности информации;
обеспечение авторских прав.

Защита от разглашения сводится в общем плане к разработке перечня сведений, составляющих коммерческую тайну предприятия. Эти сведения должны быть доведены до каждого сотрудника, допущенного к ним, с обязательством этого сотрудника сохранять коммерческую тайну. Одним из важных мероприятий является система контроля за сохранностью коммерческих секретов.

Защита от утечки конфиденциальной информации сводится к выявлению, учету и контролю возможных каналов утечки в конкретных условиях и к проведению организационных, организационно-технических и технических мероприятий по их ликвидации.

Защита от несанкционированного доступа к конфиденциальной "формации обеспечивается путем выявления, анализа и контроля возможных способов несанкционированного доступа и проникновения к источникам конфиденциальной информации и реализацией организационных, организационно-технических и технических мероприятий по противодействию НСД.

На практике в определенной степени все мероприятия по использованию технических средств защиты информации подразделяются на три группы:

организационные (в части технических средств);
организационно-технические;
технические.

Организационные мероприятия - это мероприятия ограничительного характера, сводящиеся основном, к регламентации доступа и использования технических средств обработки информации. Они, как правило, проводятся силами самой организации путем использования простейших организационных мер.

В общем плане организационные мероприятия предусматривают проведение следующих действий:

определение границ охраняемой зоны (территории);
определение технических средств, используемых для обработки конфиденциальной информации в пределах контролируемой территории;
определение "опасных", с точки зрения возможности образования каналов утечки

информации, технических средств и конструктивных особенностей зданий и сооружений;
выявление возможных путей проникновения к источникам конфиденциальной информации со стороны злоумышленников;
реализация мер по обнаружению, выявлению и контролю за обеспечением защиты информации всеми доступными средствами.

Организационные мероприятия выражаются в тех или иных ограничительных мерах. Можно выделить такие ограничительные меры, как территориальные, пространственные и временные.

Территориальные ограничения сводятся к умелому расположению источников на местности или в зданиях и помещениях, исключающих подслушивание переговоров или перехват сигналов радиоэлектронных средств.

Пространственные ограничения выражаются в выборе направлений излучения тех или иных сигналов в сторону наименьшей возможности их перехвата злоумышленниками.

Временные ограничения проявляются в сокращении до минимума времени работы технических средств, использовании скрытых методов связи, шифровании и других мерах защиты.

Одной из важнейших задач организационной деятельности является определение состояния технической безопасности объекта, его помещений, подготовка и выполнение организационных мер, исключающих возможность неправомерного овладения конфиденциальной информацией, воспрещение ее разглашения, утечки и несанкционированного доступа к охраняемым секретам.

Организационно-технические мероприятия обеспечивают блокирование разглашения и утечки конфиденциальных сведений через технические средства обеспечения производственной и трудовой деятельности, а также противодействие техническим средствам промышленного шпионажа с помощью специальных технических средств, устанавливаемых на элементы конструкций зданий, помещений и технических средств, потенциально образующих каналы утечки информации. В этих целях возможно использование:

технических средств пассивной защиты, например фильтров, ограничителей и тому подобных средств развязки акустических, электрических и электромагнитных систем защиты сетей телефонной связи, энергоснабжения, радио- и часофикации и др.;
технических средств активной защиты: датчиков акустических шумов и электромагнитных помех.

Организационно-технические мероприятия по защите информации можно подразделить на пространственные, режимные и энергетические.

Пространственные меры выражаются в уменьшении ширины диаграммы направленности, ослаблении боковых и заднего лепестков диаграммы направленности излучения радиоэлектронных средств (РЭС).

Режимные меры сводятся к использованию скрытых методов передачи информации по средствам связи: шифрование, квазипеременные частоты передачи и др.

Энергетические - это снижение интенсивности излучения и работа РЭС на пониженных мощностях.

Технические мероприятия - это мероприятия, обеспечивающие приобретение, установку и использование в процессе производственной деятельности специальных, защищенных от побочных излучений (безопасных) технических средств или средств, ПЭМИН которых не превышают границу охраняемой территории.

Технические мероприятия по защите конфиденциальной информации можно подразделить на скрытие, подавление и дезинформацию.

Скрытие выражается в использовании радиомолчания и создании пассивных помех приемным средствам злоумышленников.

Подавление - это создание активных помех средствам злоумышленников.

Дезинформация - это организация ложной работы технических средств связи и обработки информации; изменение режимов использования частот и регламентов связи; показ ложных демаскирующих признаков деятельности и опознавания.

Защитные меры технического характера могут быть направлены на конкретное техническое устройство или конкретную аппаратуру и выражаются в таких мерах, как отключение аппаратуры на время ведения конфиденциальных переговоров или использование тех или иных защитных устройств типа ограничителей, буферных средств, фильтров и устройств зашумления.

1.2. Характеристика защитных действий

Защитные действия ориентированы на пресечение разглашения, защиту информации от утечки и противодействия несанкционированному доступу.

Защитные действия, способы и мероприятия по обеспечению информационной безопасности можно классифицировать по основным характеристикам и объектам защиты по таким параметрам, например, как ориентация, характер угроз, направления, способы действий, охват, масштаб и др.

Защитные действия по ориентации можно классифицировать как действия, направленные на защиту персонала, материальных и финансовых средств и

информации как ресурса.

По направлениям - это правовая, организационная и инженерно-техническая защита.

По способам - это предупреждение, выявление, обнаружение, пресечение и восстановление.

По охвату защитные меры могут быть ориентированы на защиту территории фирмы, зданий, отдельных (выделенных) помещений, конкретных видов аппаратуры или технических средств и систем или отдельных элементов зданий, помещений, аппаратуры, опасных с точки зрения несанкционированного доступа к ним или оборудования каналов утечки информации.

Применение защитных мер можно рассматривать и в пространственном плане. Так, например, известно, что распространение (разглашение, утечка или НСД) осуществляется от источника информации через среду к злоумышленнику.

Источником информации могут быть люди, документы, технические средства, отходы и др. Носителем информации может быть либо поле (электромагнитное, акустическое), либо вещество (бумага, материал, изделие и т.д.). Средой является воздушное пространство, жесткие среды (стены, коммуникации).

Злоумышленник обладает необходимыми средствами приема акустической и электромагнитной энергии, средствами воздушного наблюдения и возможностью обрабатывать материально-вещественные формы представления информации.

Чтобы исключить неправомерное овладение конфиденциальной информацией, следует локализовать (выключить, ослабить сигнал, зашифровать и др.) источник информации.

С увеличением масштабов распространения и использования ПЭВМ и информационных сетей усиливается роль различных факторов, вызывающих утечку, разглашение и несанкционированный доступ к информации. К ним относятся:

несанкционированные и злоумышленные действия персонала и пользователя;
ошибки пользователей и персонала;
отказы аппаратуры и сбои в программах;
стихийные бедствия, аварии различного рода и опасности.

В соответствии с этими основными целями защиты информации в ПЭВМ и информационных сетях являются:

обеспечение юридических норм и прав пользователей в отношении ДОСТУПА к информационным и другим сетевым ресурсам, предусматривающее административный надзор за информационной деятельностью, включая меры

четкой персональной ответственности за соблюдение правил пользования и режимов работы;

предотвращение потерь и утечки информации, перехвата и вмешательства на всех уровнях, для всех территориально разделенных объектов;

обеспечение целостности данных на всех этапах и фазах их преобразования и сохранности средств программного обеспечения.

В связи с тем, что информационная сеть, в отличие от автономной ПЭВМ, является территориально распределенной системой, она требует принятия специальных мер и средств защиты. Средства защиты должны предотвращать:

определение содержания передаваемых сообщений;
внесение изменений в сообщения;
необоснованный отказ в доступе;
несанкционированный доступ;
ложную инициализацию обмена;
возможность измерения и анализа энергетических и других характеристик информационной системы.

Если это нецелесообразно или невозможно, то нарушить информационный контакт можно за счет использования среды распространения информации. Например, при почтовой связи использовать надежного связного и доставить почтовое отправление абоненту, полностью исключив возможность несанкционированного доступа к нему со стороны. Или исключить возможность подслушивания путем использования специального помещения, надежно защищенного о; такого вида НСД. И, наконец, можно воздействовать на злоумышленника или на его средства путем постановки активных средств воздействия (помехи).

В каждом конкретном случае реализации информационного контакта используются и свои специфические способы воздействия как на источник, так и на среду и на злоумышленника. В качестве примера рассмотрим матрицу, характеризующую взаимосвязь целей защиты информации и механизмов ее защиты в процессе телекоммуникационного обмена в распределенных автоматизированных системах. Одновременно на ней отражены и защитные возможности тех или иных механизмов.

Заключение

Информация - это ресурс. Потеря конфиденциальной информации приносит моральный или материальный ущерб.

Условия, способствующие неправомерному овладению конфиденциальной информацией, сводятся к ее разглашению, утечке и несанкционированному доступу к ее источникам.

В современных условиях безопасность информационных ресурсов может быть обеспечена только комплексной системной защиты информации.

Комплексная система защиты информации должна быть: непрерывной, плановой, целенаправленной, конкретной, активной, надежной и др.

Система защиты информации должна опираться на систему видов собственного обеспечения, способного реализовать ее функционирование не только в повседневных условиях, но и критических ситуациях.

Многообразие условий, способствующих неправомерному овладению конфиденциальной информацией, вызывает необходимость использования не менее многообразных способов, сил и средств для обеспечения информационной безопасности,

Способы обеспечения информационной безопасности должны быть ориентированы на упреждающий характер действий, направляемых на заблаговременные меры предупреждения возможных угроз коммерческим секретам.

Основными целями защиты информации являются обеспечение конфиденциальности, целостности, полноты и достаточности информационных ресурсов.

Обеспечение информационной безопасности достигается организационными, организационно-техническими и техническими мероприятиями, каждое из которых обеспечивается специфическими силами, средствами и мерами, обладающими соответствующими характеристиками.

Совокупность способов обеспечения информационной безопасности может быть подразделена на общие и частные, применение которых обусловливается масштабностью защитных действий.