1 Основные положения теории защиты информации

В начале 90-х годов группой ВУЗов были проведены исследования по проблеме безопасности информации По их результатам сформулированы основные теоретические положения, отражающие принципиальные подходы в решении вопросов защиты информации:защита информации (ЗИ) в современных системах ее обработки должна быть комплексной как по целям защиты, так и по используемым средствам;организация защиты должна осуществляться в соответствии с четкой стратегической установкой;ЗИ в любой обстановке, в любых условиях должна строиться на основе единого концептуально-методологического базиса, причем в этом базисе должен содержаться механизм, гарантирующий достижение необходимого уровня защиты;Комплексный подход к решению задач защиты Очевидно, что применительно к проблеме ЗИ речь должна идти о всеобщей комплексности, что обусловлено устойчивыми тенденциями развития систем и процессов обработки информацииК таким тенденциям развития систем и процессов обработки информации в организациях следует отнести:все более интенсивное сращивание традиционных и автоматизированных технологий обработки информации (обычного и электронного документооборота); Инструментальная комплексность предполагает одновременное и скоординированное привлечение для решения задач защиты нескольких служб, структурных подразделений, их сил и средствРешение задач защиты в соответствии с четкой стратегической установкой Стратегия защиты должна обеспечивать заданное распределение защитных ресурсов, по объектам защиты (по группам носителей информации и информационным коммуникациям) Размер ресурсов на защиту информации может быть ограничен определенным пределом, либо определяться условием достижения выбранного уровня защиты В первом случае задача решается так, чтобы при выделенных ресурсах обеспечивался максимально возможный уровень защитыОтметим, что существуют сложности с определением формального критерия защищенности данных (уровня защиты) Основная причина этого заключается в том, что процессы ЗИ зависят от большого числа случайных и трудно предсказуемых факторов Это предполагает разработку указанного критерия по вероятностной схеме Набор стратегий по защите информации, в сочетании с вероятностными оценками и позволяет преодолеть указанную сложность Количество различных стратегий должно быть небольшим, но и в то же время достаточно полно отображать гамму потенциально возможных ситуаций

2 Угрозы безопасности информации

Для того чтобы определить угрозы, от которых необходимо обезопасить информацию, нужно определить объекты защиты Ведь информация — это некоторые данные, носителями которых могут быть как материальные, так и нематериальные объекты К примеру, носителями конфиденциальной информации могут быть документы, технические средства обработки и хранения информации и даже люди  
   
 Документационными носителями информации могут быть проекты, бизнес-планы, техническая документация, контракты и договора, а также картотеки отдела кадров (персональные данные) и отдела по работе с клиентами Отличительной их особенностью является зафиксированность данных на материальном объекте — бумаге  
   
 Техническими средствами обработки и хранения информации являются персональные компьютеры, ноутбуки, серверы, сканеры, принтеры, а также съемные носители (переносные жесткие диски, флеш-карты, CD-диски, дискеты) и тп Информация в технических средствах хранится и обрабатывается в цифровом виде Зачастую конфиденциальные данные отправляются через Интернет, например, по электронной почте В сети они могут быть перехвачены злоумышленниками  
 Люди также могут быть «носителями» информации Например, сотрудники компании, которые имеют или могут иметь доступ к конфиденциальной информации Таких людей называют инсайдерами Инсайдер необязательно является злоумышленником, но в любой момент может им стать Кроме того несанкционированный доступ к конфиденциальной информации могут получить посетители, клиенты или партнеры, а также обслуживающий персонал  
 Теперь, когда мы понимаем, что нужно защищать, можно перейти непосредственно к рассмотрению угроз Они могут заключаться как в нарушении конфиденциальности, так и в нарушении достоверности, целостности и доступности информации Нарушением конфиденциальности является утечка данных, несанкционированный доступ или разглашение информации Нарушение достоверности информации — это фальсификация данных или подделка документов Искажение, ошибки при передаче информации, потери части данных являются нарушением целостности информации

3 Основные свойства информации

В литературе можно найти достаточно много определений термина «информация», отражающих различные подходы к толкованию этого понятия В «Федеральный закон Российской Федерации от 27 июля 2006 г N 149-ФЗ Об информации, технологиях и о защите информации» (http://wwwrgru/2006/07/29/informacia-dok д Сведения — это знания, выраженные в сигналах, сообщениях, известиях, уведомлениях и т д Каждого человека в мире окружает море информации различных видов Несмотря на то, что единого строгого определения информации не существует, имеется возможность описать этот термин через характерные свойства: дуализм(двойственность), достоверность, полнота, адекватность, доступность и актуальность Информация содержится везде Дерево содержит собственную генетическую информацию, и только благодаря этой информации от семечки берёзы вырастает только берёза Для деревьев источником информации является воздух, именно по состоянию воздуха дерево может определить время распускания почек Перелётные птицы знают свой маршрут перелёта, и каждая стая идёт только своим заданным в генах маршрутом Стремление зафиксировать, сохранить надолго свое восприятие информации было всегда свойственно человеку Мозг человека хранит множество информации и использует для хранения её свои способы, основа которых — двоичный код, как и у компьютеров Человек всегда стремился иметь возможность поделиться своей информацией с другими людьми и найти надёжные средства для её передачи и долговременного хранения Для этого в настоящее время изобретено множество способов хранения информации на внешних (относительно мозга человека) носителях и её передачи на огромные расстояния Основные виды информации по её форме представления, способам её кодирования и хранения, что имеет наибольшее значение для информатики, это: Существуют также виды информации, для которых до сих пор не изобретено способов их кодирования и хранения — это тактильная информация, передаваемая ощущениями, органолептическая, передаваемая запахами и вкусами и др Для передачи информации на большие расстояния первоначально использовались кодированные световые сигналы, с изобретением электричества — передача закодированного определенным образом сигнала по проводам, позднее — с использованием радиоволн

4 Политика безопасности

Политика безопасности организации (англ organizational security policies) — совокупность документированных руководящих принципов, правил, процедур и практических приёмов в области безопасности, которые регулируют управление, защиту и распределение ценной информации Политика безопасности зависит: Существуют две системы оценки текущей ситуации в области информационной безопасности на предприятии: «исследование снизу вверх» и «исследование сверху вниз» Политика безопасности организации (англ organizational security policies) — совокупность руководящих принципов, правил, процедур и практических приёмов в области безопасности, которые регулируют управление, защиту и распределение ценной информацииПолитика безопасности зависит:Существуют две системы оценки текущей ситуации в области информационной безопасности на предприятии Они получили образные названия «исследование снизу вверх» и «исследование сверху вниз»Первый метод достаточно прост, требует намного меньших капитальных вложений, но и обладает меньшими возможностями Он основан на известной схеме : «Вы — злоумышленник Ваши действия?» То есть служба информационной безопасности, основываясь на данных о всех известных видах атак, пытается применить их на практике с целью проверки, возможна ли такая атака со стороны реального злоумышленникаМетод «сверху вниз» представляет собой, наоборот, детальный анализ всей существующей схемы хранения и обработки информации Первым этапом этого метода является, как и всегда, определение, какие информационные объекты и потоки необходимо защищать Далее следует изучение текущего состояния системы информационной безопасности с целью определения, что из классических методик защиты информации уже реализовано, в каком объеме и на каком уровне На третьем этапе производится классификация всех информационных объектов на классы в соответствии с ее конфиденциальностью, требованиями к доступности и целостности (неизменности)На этапе анализа таблицы рисков задаются некоторым максимально допустимым риском, например значением 7 Сначала проверяется каждая строка таблицы на не превышение риска этого значения Если такое превышение имеет место, значит, данная строка – это одна из первоочередных целей разработки политики безопасности Затем производится сравнение удвоенного значения (в нашем случае 7\*2=14) с интегральным риском (ячейка «Итого»)

5 Модели безопасности

42 Модели безопасности и их применениеМетод формальной разработки системы опирается на модель безопасности (модель управления доступом, модель политики безопасности) Целью этой модели является выражение сути требований по безопасности к данной системе Она определяет потоки информации, разрешенные в системе, и правила управления доступом к информацииМодель позволяет провести анализ свойств системы, но не накладывает ограничений на реализацию тех или иных механизмов защиты Так как она является формальной, возможно осуществить доказательство различных свойств безопасности системыХорошая модель безопасности обладает свойствами абстрактности, простоты и адекватности моделируемой системеМодель дискреционного доступа (DAC)В дискреционной модели контролируется доступ субъектов (пользователей или приложений) к объектам, представляющим собой различные информационные ресурсы: файлы, приложения, устройства вывода и т дДля каждого объекта существует субъект-владелец, который сам определяет тех, кто имеет доступ к объекту, а также разрешенные операции доступа Основными операциями доступа являются READ (чтение), WRITE (запись) и EXECUTE (выполнение, имеет смысл только для программ) В модели дискреционного доступа для каждой пары субъект-объект устанавливается набор разрешенных операций доступаМодель безопасности белла-ЛаПадулыОдна из наиболее известных моделей безопасности – модель Белла-ЛаПадулы (модель мандатного управления доступом) В ней определено множество понятий, связанных с контролем доступа Даются определения субъекта, объекта и операции доступа, а также математический аппарат для их описания Эта модель в основном известна двумя основными правилами безопасности: одно относится к чтению, а другое – к записи данных (Рис 2)Модель безопасности белла-ЛаПадулыОдна из наиболее известных моделей безопасности – модель Белла-ЛаПадулы (модель мандатного управления доступом) В ней определено множество понятий, связанных с контролем доступа Даются определения субъекта, объекта и операции доступа, а также математический аппарат для их описания Эта модель в основном известна двумя основными правилами безопасности: одно относится к чтению, а другое – к записи данных (Рис 2)

6 Дискреционный контроль доступа

Избирательное управление доступом (англ discretionary access control, DAC) — управление доступом субъектов к объектам на основе списков управления доступом или матрицы доступа Также используются названия дискреционное управление доступом, контролируемое управление доступом и разграничительное управление доступом Возможны несколько подходов к построению дискреционного управления доступом: Избирательное управление доступом является основной реализацией разграничительной политики доступа к ресурсам при обработке конфиденциальных сведений, согласно требованиям к системе защиты информации Избирательное управление доступом (англ Discretionary access control, DAC) — управление доступом субъектов к объектам на основе или матрицы доступаДля каждой пары (субъект — объект) должно быть задано явное и недвусмысленное перечисление допустимых типов доступа (читать, писать и т д), то есть тех типов доступа, которые являются санкционированными для данного субъекта (индивида или группы индивидов) к данному ресурсу (объекту)[1]Возможны и смешанные варианты построения, когда одновременно в системе присутствуют как владельцы, устанавливающие права доступа к своим объектам, так и суперпользователь, имеющий возможность изменения прав для любого объекта и (или) изменения его владельца Именно такой смешанный вариант реализован в большинстве операционных систем, например, в классических Windows семейства NTИзбирательное управление доступом является основной реализацией разграничительной политики доступа к ресурсам при обработке конфиденциальных сведений, согласно требованиям к системе защиты информацииКонтроль доступа (информатика) — Контроль доступа – функция открытой системы, обеспечивающая технологию безопасности, которая разрешает или запрещает доступ к определенным типам данных, основанную на идентификации объекта, которому нужен доступ, и объекта данных являющегося… …   ВикипедияКонтроль доступа — является одной из самых важных элементов защиты вашего ПК и Информации на нем Доступ к защищенной информации должен быть ограничен, чтобы только люди, которые имеют право доступа, могли получать эту информацию Компьютерные программы и во многих …   Википедия

7 Модель распространения прав доступа Take-Grant

Модель Take-Grant (от англ Модель представляет всю систему как направленный граф, где узлы — либо объекты, либо субъекты Дуги между ними маркированы, и их значения указывают права, которые имеет объект или субъект (узел) В модели доминируют два правила: «брать» и «давать»Презентация на тему Презентация на тему Расширенная модель Take-Grant, предмет презентации: Информатика Этот материал содержит 27 слайдов Красочные слайды и илюстрации помогут Вам заинтересовать свою аудиторию Для просмотра воспользуйтесь проигрывателем, если материал оказался полезным для Вас - поделитесь им с друзьями с помощью социальных кнопок и добавьте наш сайт презентаций ThePresentationru в закладки!МОДЕЛЬ TAKE-GRANT Модель распространения прав доступа Take-Grant, предложенная в 1976 г, используется для анализа систем дискреционного разграниче­ния доступа, в первую очередь для анализа путей распространения прав доступа в таких системах В качестве основных элементов модели ис­пользуются граф доступов и правила его преобразования Цель модели - дать ответ на вопрос о возможности получения прав доступа субъектом системы на объект в состоянии, описываемом графом доступов В на­стоящее время модель Take-Grant получила продолжение как расширен­ная модель Take-Grant, в которой рассматриваются пути возникнове­ния информационных потоков в системах с дискреционным разграничени­ем доступа Модель распространения прав доступа Take-Grant, предложенная в 1976 г, используется для анализа систем дискреционного разграниче­ния доступа, в первую очередь для анализа путей распространения прав доступа в таких системах В качестве основных элементов модели ис­пользуются граф доступов и правила его преобразования Цель модели - дать ответ на вопрос о возможности получения прав доступа субъектом системы на объект в состоянии, описываемом графом доступов В на­стоящее время модель Take-Grant получила продолжение как расширен­ная модель Take-Grant, в которой рассматриваются пути возникнове­ния информационных потоков в системах с дискреционным разграничени­ем доступа

8 Модели мандатного контроля и управления доступом

Мандатное управление доступом (англ Mandatory access control, MAC) — разграничение доступа субъектов к объектам, основанное на назначении метки конфиденциальности для информации, содержащейся в объектах, и выдаче официальных разрешений (допуска) субъектам на обращение к информации такого уровня конфиденциальности Также иногда переводится как Принудительный контроль доступа Это способ, сочетающий защиту и ограничение прав, применяемый по отношению к компьютерным процессам, данным и системным устройствам и предназначенный для предотвращения их нежелательного использования Согласно требованиям ФСТЭК, мандатное управление доступом или «метки доступа» являются ключевым отличием систем защиты государственной тайны РФ старших классов 1В и 1Б от младших классов защитных систем на классическом разделении прав по матрице доступа Мандатная модель управления доступом, помимо дискреционной и ролевой, является основой реализации разграничительной политики доступа к ресурсам при защите информации ограниченного доступа При этом данная модель доступа практически не используется «в чистом виде», обычно на практике она дополняется элементами других моделей доступа Самое важное достоинство заключается в том, что пользователь не может полностью управлять доступом к ресурсам, которые он создаёт Проблема разграничения доступа к информации существовала испокон веков Полководцы хотели сберечь свои планы о наступлении, торговцы скрывали свои доходы, а революционеры - заговоры Перед всеми ними стоял вопрос: как избежать утечки информации? Полного решения этой проблемы не существует и по сей день Однако, некоторые современные стратегии управления доступом обеспечивают очень высокий уровень безопасности информацииС приходом эпохи компьютеров озвученная проблема встала особо остро В поисках решения было разработано множество систем управления доступом, которые использовали и новые и старые знания и наработки в этой области На сегодняшний день наиболее надежной с точки зрения защиты информации считается мандатная система управления доступом, о которой мы и поговорим в этой статье

9 Модели контроля целостности

Рассмотрим модели безопасности, контролирующие целостность информации В частности, модели Биба, использующиеся для синтеза механизмов контроля целостности информации в системе, а также модель Кларка – Вилсона (КВМ), которая является примером неформального выражения политики безопасности Последняя модель сформулирована в виде набора неформальных правил, и хотя в литературе она названа моделью безопасности, ее скорее можно назвать политикой контроля целостностиКен Биба в середине семидесятых годов прошлого века сделал два наблюдения Они были последовательно внесены в модель безопасности, которая с тех пор называется моделью целостности Биба (или просто моделью Биба) В контексте разговора о моделях контроля целостности запись наверх может представлять угрозу в том случае, если субъект с низким уровнем безопасности искажает или уничтожает данные в объекте, лежащем на более высоком уровне Поэтому, исходя из задач целостности, можно потребовать, чтобы такая запись была запрещена Кроме того, можно рассматривать чтение снизу как поток информации, идущий из объекта нижнего уровня и нарушающий целостность субъекта высокого уровняБиба выразил свою модель таким же способом, каким была выражена БЛМ, за тем исключением, что правила его модели являются полной противоположностью правилам БЛМ Возможны три вариации модели Биба: мандатная модель целостности, модель понижения уровня субъекта и модель понижения уровня объекта Фактически, общий термин «модель Биба» используется для обозначения любой или сразу всех трех моделейЕе часто называют инверсией БЛМ Это довольно точное название, поскольку основные правила этой модели просто переворачивают правила БЛМ Мы будем ссылаться на эти правила как «нет чтения снизу» (NRD) и «нет записи наверх» (NWU) и определим их в терминах субъектов, объектов и нового типа уровней безопасности – уровней целостности, над которыми может быть введено отношение преобладанияПравило NRD мандатной модели целостности Биба определяется как запрет субъектам на чтение информации из объекта с более низким уровнем целостности Правило NWU мандатной модели целостности Биба определяется как запрет субъектам на запись информации в объект с более высоким уровнем целостности

10 Ролевые модели доступа

Ролевая модель доступа – это основополагающий документ, четко определяющий необходимый набор прав доступа ко всем элементам корпоративной ИС для каждой должности в организации Именно на основании данных, заложенных в ролевую модель, IDM может автоматически назначать права доступа новым сотрудникам или проводить аудит прав доступа, выявляя отличия реальных наборов прав в конечных ИТ-системах с эталонными наборами, заложенными в ролевой модели  
   
 Но даже пройдя этот сложный и долгий путь и создав подробную ролевую модель, команда проекта сталкивалась со второй, не менее сложной задачей – ее утверждением у ключевых руководителей организации Именно на этом шаге во всей красе проявляются классические противостояния между различными подразделениями организации и разрыв в понимании бизнес-процессов между руководством и подчиненными И дело не только в демонстрации своего влияния, хотя и этот фактор присутствует Типична ситуация, когда высокопоставленные начальники крайне слабо представляют себе, как организованы реальные рабочие процессы, но при этом не могут отказаться от соблазна попробовать оптимизировать и улучшить принесенный им на утверждение документ В итоге утверждение ролевой модели или вполне сопоставимо по срокам с ее созданием, или занимает даже больше времени Да и процесс согласования такой модели не занимает много времени, так как при ее создании отсутствовал какой-либо субъективизм исполнителя, система автоматически обобщила те права, которые уже были у сотрудников к настоящему моменту, и не имеет смысла их оспаривать  
   
 Однако нужно понимать, что после запуска IDM-системы с базовыми ролями работа с ролевой моделью не заканчивается Теперь, когда IDM-система нормально работает и приносит пользу, можно спокойно и постепенно оптимизировать ролевую модель, а начинать эту работу лучше всего с анализа всех тех прав, которые были оставлены в ролевой модели как исключения Если их необходимость подтверждается, их можно включить в базовые роли, а если нет, – заблокировать

11 Идентификация и аутентификация в информационных системах

Системы идентификации, аутентификации и авторизацииДля защиты конфиденциальной информации на предприятии также применяются разграничение прав доступа для различных групп пользователей Для определения прав доступа к определенным ресурсам и управления этим доступам применяются различные схемы авторизации Идентификация и аутентификация также применяются для защиты информационной безопасностиИнформационная безопасностьИнформационная безопасность Сегодня мы узнаем, что такое идентификация, аутентификация, авторизация и в чем разница между этими понятиями Идентификация — это процедура распознавания субъекта по его идентификатору (проще говоря, это определение имени, логина или номера)Идентификация выполняется при попытке войти в какую-либо систему (например, в операционную систему или в сервис электронной почты)После идентификации производится аутентификация:Ну как, понятно, что такое аутентификация? Если остались вопросы, можно задать их в комментариях, но перед этим разберемся еще с одним терминомРазберемся на примерах, что же это за загадочная авторизация:Инфографика: 1 — Идентификация; 2 — Аутентификация; 3 — Авторизация Инфографика: 1 — Идентификация; 2 — Аутентификация; 3 — АвторизацияИтак, сегодня вы узнали, что такое идентификация, аутентификация и авторизацияСергей, спасибо вам за урок Ох, и хороши же наши старые мультики! Впервые смотрела его под таким углом Наверное, запуталась, перебивали несколько раз…, поэтому подсчеты могут быть ошибочными У меня получились такие результаты: 1 Идентификация (кто там, ты кто) — 8; 2Здравствуйте! Я правильно поняла, что грубейшую ошибку совершила бабушка, которая нарушила последовательность, а именно- пропустила аутентификацию ( процедуру проверки подлинности идентификата?)Следовательно: Идентификация- авторизация Все, волк в домеОчень познавательно не задумывался над понятиями -Идентификация, Аутентификация и Авторизация Мне очень интересно и главное полезно это знать, а значит это реально поможет в освоении компьютера и не только

12 Аудит информационной безопасности

Информация — один из ключевых активов любого бизнеса или организации Для безопасной работы с большим объемом данных компании обязаны выстраивать системы управления информационной безопасностью (СУИБ)В современном мире активно развиваются механизмы по краже данных или использованию незаконно полученного доступа к ресурсам организации для извлечения прибыли Поэтому от организаций требуется постоянное совершенствование СУИБ Это становится причиной постоянного роста непрофильных затрат на поиск и обучение специалистов по информационной безопасности (ИБ), покупке дорогостоящих средств информационной защиты, а также поддержания всей системы информационной защиты в актуальном состоянии Зачастую бизнесу приходится думать о работе безопасности в круглосуточном режиме, что еще больше увеличивает вложения в человеческие и инфраструктурные ресурсы Чтобы СУИБ были эффективны, нужно выполнять аудиторские проверки информационной безопасности Какие виды аудита бывают, зачем и когда их стоит проводить — рассказываем в статьеАудит информационной безопасности — мероприятия для проверки текущего состояния защиты ИТ-инфраструктуры, выявления потенциальных угроз и уязвимостей Аудиторские проверки могут проводиться в отношении корпоративных сетей, отдельных устройств, сайтов, приложений, программ, серверов разных масштабов и процессов Аудит информационной безопасности нужен не только тем компаниям, которые работают с конфиденциальными данными Стабильность и надежность СУИБ также важны, например, для интернет-магазинов, сервисов логистики, информационных ресурсовМожно выделить внутренний и внешний аудит информационной безопасности Внутренний аудит направлен на выявление внутренних проблем, несоответствий и уязвимостей в системе безопасности Он помогает обнаружить недостатки СУИБ, повлекшие за собой потерю данных, финансов, репутации и другой ущерб Внутренний аудит бывает повседневным или проводимым по заранее согласованному плану специально определенным подразделением За повседневный аудит отвечают сотрудники, связанные с процессом определения негативного воздействия на инфраструктуру организации Среди них: инженеры, отвечающие за эксплуатацию инфраструктуры, сотрудники подразделений информационной безопасности, службы мониторинга, защиты активов и другие Они отслеживают изменения в основных показателях, присущих информации (целостность, доступность, конфиденциальность), в своей зоне ответственности и оперативно вносят коррективы для разрешения последствий

13 Уязвимости информационных систем

52 Общая характеристика уязвимостей информационнойУязвимость информационной системы персональных данных - недостаток или слабое место в системном или прикладном программном (программно-аппаратном) обеспечении автоматизированной информационной системы, которые могут быть использованы для реализации угрозы безопасности персональных даннымПричинами возникновения уязвимостей являются:преднамеренные действия по внесению уязвимостей в ходе проектирования и разработки программного (программно-аппаратного) обеспечения;несанкционированные неумышленные действия пользователей, приводящие к возникновению уязвимостей;Классификация основных уязвимостей ИСПДн приведена на рисунке 4 │Классификация уязвимостей│Рисунок 4 Классификация уязвимостейНиже представлена общая характеристика основных групп уязвимостей ИСПДн, включающих:Защита информации1 РАЗРАБОТАН Обществом с ограниченной ответственностью "Центр безопасности информации" (ООО "ЦБИ")2 ВНЕСЕН Техническим комитетом по стандартизации ТК 362 "Защита информации"Настоящий стандарт распространяется на деятельность по защите информации, связанную с выявлением и устранением уязвимостей ИС, при создании и эксплуатации ИСНастоящий стандарт устанавливает классификацию уязвимостей информационных систем (ИС) Настоящий стандарт направлен на совершенствование методического обеспечения определения и описания угроз безопасности информации при проведении работ по защите информации в ИСНастоящий стандарт не распространяется на уязвимости ИС, связанные с утечкой информации по техническим каналам, в том числе уязвимости электронных компонентов технических (аппаратных и аппаратно-программных) средств ИСГОСТ Р 50922 Защита информации Основные термины и определения31 информационная система: Совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств32 компонент информационной системы: Часть информационной системы, включающая некоторую совокупность информации и обеспечивающих ее обработку отдельных информационных технологий и технических средств

14 Компьютерные и сетевые атаки

Любая компания в своей деятельности сегодня использует широкие возможности, которые дает интернет Однако вместе с возможностями всемирная сеть приносит множество угроз информационной безопасности Реализация этих угроз может приводить к значительному материальному и репутационному ущербу для бизнеса Поэтому важно иметь представление об основных типах сетевых атак и способах защиты от нихВиды сетевых атак и их последствия имеют значительные отличия друг от друга Современная классификация угроз проводится по следующим параметрам:Рассмотрим подробнее основные виды сетевых атак по этим категориямВиды сетевых атак по характеру воздействия на атакуемую сеть можно разделить на активные и пассивныеВ зависимости от цели различают виды сетевых атак, направленных на нарушение:Существуют разные условия начала воздействия В том числе можно выделить такие типы сетевых атак по этому критерию:В качестве примеров наиболее распространенных сетевых атак можно привести следующие виды воздействия:В связи с быстрым развитием информационных технологий и технических средств статичные механизмы защиты от сетевых угроз часто оказываются неэффективными Обеспечить эффективную защиту информации позволяют динамические методы, способные оперативно выявлять и устранять угрозы Работа динамических технологий строится на оценки уровня подозрительности действий в сети со стороны определенной службы или процессаДля защиты сетей от внешних угроз могут применяться следующие основные методы и технологии:Разнообразие видов сетевых атак, которым могут подвергаться корпоративные и частные сети, требует выработки эффективных мер по их защите Такие меры должны разрабатываться и применяться заблаговременно Эффективная защита от угроз поможет сохранить неприкосновенными конфиденциальные данные и обеспечить стабильную работу сети Благодаря этому многократно окупаются расходы, понесенные на внедрение такой защитыНа сегодняшний день известны следующие виды сетевых атак:Защита состоит в том, чтобы обнаружить и устранить уязвимости Также используются неисполнимые буфера, но этот метод способен предотвратить только те атаки, в которых применяется код

15 Общая характеристика технических каналов утечки информации

Под техническим каналом утечки информации (ТКУИ) понимают совокупность источника информации (передатчика), линии связи (физической среды – канал с шумами), по которой распространяется информационный сигнал, и технических средств перехвата информации (приемника) Для понимания физического смысла ТКУИ  и основных вопросов защиты информации  (ЗИ) рассмотрим элементарную модель произвольного технического канала утечки (Рис 1)Общая классификация ТКУИ включает следующие виды:Каналы утечки информации — методы и пути утечки информации из информационной системы; паразитная (нежелательная) цепочка носителей информации, один или несколько из которых являются (могут быть) правонарушителем или его специальной аппаратурой Играют основную роль в защите информации, как фактор информационной безопасности Все каналы утечки данных можно разделить на косвенные и прямые Косвенные каналы не требуют непосредственного доступа к техническим средствам информационной системы Прямые соответственно требуют доступа к аппаратному обеспечению и данным информационной системы Примеры косвенных каналов утечки: Примеры прямых каналов утечки: Каналы утечки информации можно также разделить по физическим свойствам и принципам функционирования: В зависимости от вида каналов связи технические каналы перехвата информации можно разделить[1] Технические каналы утечки информации можно разделить на естественные и специально создаваемые Виды технических каналов утечки акустической информации:[6] Акустический канал утечки информации реализуется в следующем: Акустоэлектрический канал утечки информации, особенностями которого являются: Телефонный канал утечки информации для подслушивания телефонных переговоров (в рамках промышленного шпионажа) возможен: Индуктивный способ — за счёт электромагнитной индукции, возникающей в процессе телефонных переговоров вдоль провода телефонной линии В качестве приемного устройства съёма информации используется трансформатор, первичная обмотка которого охватывает один или два провода телефонной линии

16 Теоретические основы акустики

Э Мидлер 11 Введение Распространение волн — это физическое явление, на котором основаны все методы и применения ультразвука в медицине В настоящей книге сделана попытка, исходя из физических основ, выделить принципы и практические результаты, достигнутые в этой большой области, лежащей на стыке разных наукРаспространение волн — это физическое явление, на котором основаны все методы и применения ультразвука в медицине В настоящей книге сделана попытка, исходя из физических основ, выделить принципы и практические результаты, достигнутые в этой большой области, лежащей на стыке разных наук Основы волновой физики знакомы большинству читателей книги, и с учетом этого первая глава преследует несколько целей Во-первых, она призвана напомнить читателям принятые обозначения и методологию Во-вторых, в ней мы рассмотрим ограничения и приближения, необходимые для решения некоторых задач биомедицинской акустикиОсновы волновой физики знакомы большинству читателей книги, и с учетом этого первая глава преследует несколько целей Во-первых, она призвана напомнить читателям принятые обозначения и методологию Во-вторых, в ней мы рассмотрим ограничения и приближения, необходимые для решения некоторых задач биомедицинской акустики глмедицинских диагностических приборов используются именно импульсные излучатели, генерирующие несколько периодов колебаний Уметь моделировать и описывать такой сигнал очень важно Например, известно, что продольное разрешение излучателя (в отличие от азимутального или поперечного) зависит от длительности импульса Известно также, что при излучении коротких импульсов уменьшаются боковые лепестки и изрезанность структуры поля по сравнению с непрерывной волной Боковые лепестки и изрезанность ухудшают качество изображения, так как приводят к неоднозначности цели или к снижению поперечного разрешенияВ этой главе рассматривается теоретическое описание распространения импульса, что отражается на выборе математического аппарата (в частности, используется преобразование Лапласа, а не Фурье) Ясно, что из-за большого числа независимых переменных, включаемых в описание нестационарного звукового поля при использовании более строгих теоретических методов, теряется их гибкость и наглядность Более приближенный модельный подход может оказаться достаточным для решения сложных инженерных задач, таких как описание работы решеток преобразователей в импульсном режиме Общее предположение в излагаемой теории — линейность, т е

17 Электромагнитные волны, как канал утечки информации

Существует несколько способов утечки информации, одним из которых является радиоэлектронный способ Радиоэлектронный канал утечки информации — канал, в котором носителем информации служит электромагнитное поле и электрический ток Самым информативным каналом утечки информации является радиоэлектронный канал В зависимости от источника сигнала существует 2 вида радиоэлектронного канала утечки информации В первом случае осуществляется перехват информации, которая передаётся по функциональному каналу Во втором случае каналы утечки информации специально устанавливаются злоумышленниками Каналы утечки информации — методы и пути утечки информации из информационной системы; паразитная (нежелательная) цепочка носителей информации, один или несколько из которых являются (могут быть) правонарушителем или его специальной аппаратурой Играют основную роль в защите информации, как фактор информационной безопасности Все каналы утечки данных можно разделить на косвенные и прямые Косвенные каналы не требуют непосредственного доступа к техническим средствам информационной системы Прямые соответственно требуют доступа к аппаратному обеспечению и данным информационной системы Примеры косвенных каналов утечки: Примеры прямых каналов утечки: Каналы утечки информации можно также разделить по физическим свойствам и принципам функционирования: В зависимости от вида каналов связи технические каналы перехвата информации можно разделить[1] Технические каналы утечки информации можно разделить на естественные и специально создаваемые Виды технических каналов утечки акустической информации:[6] Акустический канал утечки информации реализуется в следующем: Акустоэлектрический канал утечки информации, особенностями которого являются: Телефонный канал утечки информации для подслушивания телефонных переговоров (в рамках промышленного шпионажа) возможен: Индуктивный способ — за счёт электромагнитной индукции, возникающей в процессе телефонных переговоров вдоль провода телефонной линии В качестве приемного устройства съёма информации используется трансформатор, первичная обмотка которого охватывает один или два провода телефонной линии

18 Применение антенны в технических средствах защиты информации

Приведены концептуальные основы инженерно-технической защиты информации, ее основные принципы, классифицированы и определены основные методы и средства обеспечения информационной безопасности по каждому из возможных каналов утечки Приведены концептуальные основы инженерно-технической защиты информации, ее основные принципы, классифицированы и определены основные методы и средства обеспечения информационной безопасности по каждому из возможных каналов утечкиКлючевые слова: системы защиты информации, технические каналы утечки информации, побочные электромагнитные излучения и наводки, закладные устройства, сотовая связь, диктофоны, направленные микрофоны, телефонный канал передачи информации, экранирование, шумы, помехиПерехватом информации называется неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, приём и обработку информативных сигналов [1,3]В результате перехвата информации возможно неправомерное ознакомление с информацией илинеправомерная запись информации на носительОсобенности технических каналов утечки информации определяются физической природой информационных сигналов и характеристиками среды их распространения Общая классификация технических каналов утечки информации включает следующие виды каналов (рис1) [1,2]:- каналы утечки, обрабатываемой техническими средствами приема, обработки, хранения и передачи информации (ТСПИ);- каналы утечки речевой информации;- утечка информации при ее передаче по каналам связи;- технические каналы утечки видовой информацииТехнические каналы утечки информацииинформации ТКУИ с ТСПИТКУ видовой информацииРис 1 Общая классификация технических каналов утечки информацииТехнические каналы утечки информации, обрабатываемой ТСПИ- съем информации с использованием закладных устройств- перехват информации путем «высокочастотного облучения» ТСПИ5 Съём информации с использованием закладных устройствЗакладные устройства, внедряемые в СВТ, по виду перехватываемой информации можно разделить на [3,4]:

19 Методы и средства защиты информации от утечки по техническим каналам

Средства защиты информации по каналам ПЭМИНЗа счет побочных электромагнитных излучений и наводок (ПЭМИН), можно считывать информацию с монитора вашего компьютера (разумеется с помощью специальных технических средств) на расстоянии до 200 метров, а то и больше Также можно считывать информацию с процессора, клавиатуры, винчестера, дисковода (когда они работают, естественно) Поэтому все криптосистемы становятся почти бессмысленными если не принять соответствующих мер защитыСредства защиты акустической речевой информацииЗащита речевой (акустической) информации является одной из задач в комплексе мероприятий по обеспечению информационной безопасности объекта технической защиты информации Это связано с тем, что возможен перехват конфиденциальной информации (информации ограниченного доступа) в процессе обсуждения служебных вопросовСредства защиты от несанкционированного применения сотовых телефонов, диктофонов и радиопередатчиковПредназначены для предотвращения утечки информации за счет несанкционированного использования сотовых телефонов Также могут применяться в помещениях, где использование сотовых телефонов нежелательно (театры, залы переговоров и тп) Для дополнительной информации вы можете ознакомиться с «Политикой использования cookie-файлов»III Методы и способы защиты информацииот утечки по техническим каналам31 N 78132 Для исключения утечки персональных данных за счет побочных электромагнитных излучений и наводок в информационных системах 1 класса могут применяться следующие методы и способы защиты информации:использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;размещение объектов защиты в соответствии с предписанием на эксплуатацию;333435Защита информации от утечки по техниӯческим каналам — это комплекс органиӯзационных, организационно - технических и технических мероприятий, исключаюӯщих или ослабляющих бесконтрольный выход конфиденциальной информации за пределы контролируемой зоныЗащита информации от утечки по визуально-оптиӯческому каналу — это комплекс мероприятий, исклюӯчающих или уменьшающих возможность выхода конӯфиденциальной информации за пределы контролируеӯмой зоны за счет распространения световой энергии

20 Защита информации в проводных телефонных системах

Delphi site: daily Delphi-news, documentation, articles, review, interview, computer humorПри защите телефонных аппаратов и телефонных линий необходимо учитывать несколько аспектов:Телефонный аппарат имеет несколько элементов, имеющих способность преобразовывать акустические колебания в электрические, то есть обладающих «микрофонным эффектом» К ним относятся: звонковая цепь, телефонный и микрофонный капсюли За счет электроакустических преобразований в этих элементах возникают информационные (опасные) сигналы Способы защиты и соответствующая аппаратура защиты рассмотрены в гл9Для защиты телефонных линий используются как простые устройства, реализующие один метод защиты, так и сложные, обеспечивающие комплексную защиту линий различными методами, включая защиту от утечки информации по электроакустическому каналуНа отечественном рынке имеется большое разнообразие средств защиты Среди них можно выделить следующие: «8Р 17/Т», «81-2001», «КТЛ-3», «КТЛ-400», «Ком-3», «Цикада-М», «Прокруст» (ПТЗ-ООЗ), «Прокруст-2000», «Гром-ЗИ-6», «Протон» и дрВ аппаратуре защиты для обеспечения достаточно высокой защищенности как передаваемой информации,так и акустики помещений ,в которых расположен тлф аппарат используют активные,пассивные и комбинированные способы защитыПассивные и активные способы защиты Способы и средства пассивной защитыК наиболее широко применяемым пассивным методам защиты относятся:Возможность ограничения опасных сигналов основывается на нелинейных свойствах полупроводниковых элементов, главным образом диодов В схеме ограничителя малых амплитуд используются два встречно включенных диода На начальном этапе вольтамперной характеристики сопротивление таких диодов велико (сотни кОм и выше) Это исключает прохождение опасных сигналов малой амплитуды в телефонную линию и практически не оказывает влияние на прохождение через диоды сигналов вызова и переговоров Диодные ограничители включаются последовательно в линию звонка или непосредственно в каждую из телефонных линий и широко используются для защиты каналов утечки акустопреобразователь-ных каналов утечки информации

21 Возможности и способы несанкционированного подключения к телефонным линиям

Технологии защиты телефонных переговоров — методы и средства защиты, направленные на обеспечение конфиденциальности обмена информацией между абонентами Контроль телефонных переговоров остается одним из наиболее распространенных видов промышленного шпионажа и действий преступных элементов [1] Причины просты — низкий уровень затрат и риск реализации угроз, необязательность захода в контролируемое помещение, разнообразие способов и мест съёма информации и пр Контролировать телефонные разговоры можно на всем протяжении телефонной линии, а при использовании сотовой телефонной связи — во всей сотовой зоне Учитывая нынешнюю стоимость информации, технологии и способы защиты телефонных переговоров будут стремительно развиваться и эволюционироватьОсновой любой системы защиты информации, любого плана противодействий является знание угроз и степени их опасности[2] В настоящее время для передачи информации используют в основном КВ, УКВ, радиорелейные, тропосферные и космические каналы связи, а также кабельные и волоконно-оптические линии связи В зависимости от вида каналов связи технические каналы перехвата информации можно разделить на электромагнитные, электрические и индукционные Высокочастотные электромагнитные излучения передатчиков средств связи, модулированные информационным сигналом, могут перехватываться портативными средствами радиоразведки и передаваться в центр обработки для их обработки Данный канал перехвата информации наиболее широко используется для прослушивания телефонных разговоров, ведущихся по радиотелефонам, сотовым телефонам или по спутниковым линиям связи[3] В случае использования сигнальных устройств контроля целостности линии связи, её активного и реактивного сопротивления факт контактного подключения к ней аппаратуры разведки будет обнаружен Поэтому спецслужбы наиболее часто используют индуктивный канал перехвата информации, не требующий контактного подключения к каналам связи В данном канале используется эффект возникновения вокруг кабеля связи электромагнитного поля при прохождении по нему информационных электрических сигналов, которые перехватываются специальными индукционными датчиками Индукционные датчики используются в основном для съёма информации с симметричных высокочастотных кабелей Современные индукционные датчики способны снимать информацию с кабелей, защищенных не только изоляцией, но и двойной броней из стальной ленты и стальной проволоки, плотно обвивающих кабель

22 Возможности обнаружения подключений средств снятия информации в проводных каналах

Система защиты помещений"SEL SP-55-4A"Система является техническим средством активной защиты информации по виброакустическому каналу для объектов информатизации 1 категорииНаличие интерфейса RS-485 (опция) позволяет включать его в интегрированные комплексные системы защиты информации, где удаленное управление прибором и контроль его состояния осуществляется с ПК или автономного контроллераПрибор виброакустической защиты SI-3010 предназначен для виброакустического зашумления строительных конструкций помещения при защите речевой информации от утечки по вибрационному и акустическому каналамЛГШ-403 обеспечивает защиту путем постановки широкополосной виброакустической шумовой помехи на потенциально опасные конструкции помещений Кроме того, предусмотрена возможность установки акустического излучателя для защиты воздуховодов и вентиляционных шахт Приведены концептуальные основы инженерно-технической защиты информации, ее основные принципы, классифицированы и определены основные методы и средства обеспечения информационной безопасности по каждому из возможных каналов утечки Приведены концептуальные основы инженерно-технической защиты информации, ее основные принципы, классифицированы и определены основные методы и средства обеспечения информационной безопасности по каждому из возможных каналов утечкиКлючевые слова: системы защиты информации, технические каналы утечки информации, побочные электромагнитные излучения и наводки, закладные устройства, сотовая связь, диктофоны, направленные микрофоны, телефонный канал передачи информации, экранирование, шумы, помехиПерехватом информации называется неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, приём и обработку информативных сигналов [1,3]В результате перехвата информации возможно неправомерное ознакомление с информацией илинеправомерная запись информации на носительОсобенности технических каналов утечки информации определяются физической природой информационных сигналов и характеристиками среды их распространения Общая классификация технических каналов утечки информации включает следующие виды каналов (рис1) [1,2]:

23 Каналы утечки информации, образованные электромагнитным излучением.

Каналы утечки информации — методы и пути утечки информации из информационной системы; паразитная (нежелательная) цепочка носителей информации, один или несколько из которых являются (могут быть) правонарушителем или его специальной аппаратурой Играют основную роль в защите информации, как фактор информационной безопасности Все каналы утечки данных можно разделить на косвенные и прямые Косвенные каналы не требуют непосредственного доступа к техническим средствам информационной системы Прямые соответственно требуют доступа к аппаратному обеспечению и данным информационной системы Примеры косвенных каналов утечки: Примеры прямых каналов утечки: Каналы утечки информации можно также разделить по физическим свойствам и принципам функционирования: В зависимости от вида каналов связи технические каналы перехвата информации можно разделить[1] Технические каналы утечки информации можно разделить на естественные и специально создаваемые Виды технических каналов утечки акустической информации:[6] Акустический канал утечки информации реализуется в следующем: Акустоэлектрический канал утечки информации, особенностями которого являются: Телефонный канал утечки информации для подслушивания телефонных переговоров (в рамках промышленного шпионажа) возможен: Индуктивный способ — за счёт электромагнитной индукции, возникающей в процессе телефонных переговоров вдоль провода телефонной линии В качестве приемного устройства съёма информации используется трансформатор, первичная обмотка которого охватывает один или два провода телефонной линии В оптическом канале получение информации возможно путём: В качестве среды распространения в оптическом канале утечки информации выступают: Безвоздушное пространство, являющееся средой распространения утечки информации, возникает при наблюдении за наземными объектами с космических аппаратов К свойствам среды распространения, влияющих на длину канала утечки, относятся: Типовые варианты оптических каналов утечки информации приведены в таблице Технические средства съёма информации могут быть внедрены «противником» следующими способами:

24 Общие сведения о криптографических методах защиты информации

Криптография  
 – наука о шифрах Долгое время сведения этой предметной области были строго  
 засекречены, так как шифры  применялись, в основном, для защиты государственных  
 и военных се­кретов В настоящее время методы и средства криптографии  
 используются для обеспечения информационной безопасности не только государства,  
 но и частных лиц и организаций Дело здесь совсем не обязательно в секретах  
 Слишком много различных сведений «гуляет» по всему свету в цифровом ви­де Темпы  
 развития информационных технологий таковы, что косвенно многим уже приходилось  
 пользоваться некоторыми криптографическими средствами: шифрование электронной  
 почты, электронной подписи, интел­лектуальные банковские карточки и др  
 Естественно, что при этом основной вопрос для пользователя – обеспечивает ли  
 данное криптографическое сред­ство надежную защиту Но даже правильно  
 сформулировать этот элементар­ный вопрос непросто От какого противника  
 защищаемся? Какие возможно­сти у этого противника? Какие цели он может  
 преследовать? Как измерять надежность защиты? Список таких вопросов можно продолжить  
   
  Для  
 ответа на них пользователю необходимы знания основных понятий криптографииТемпы  
 развития информационных технологий таковы, что косвенно многим уже приходилось  
 пользоваться некоторыми криптографическими средствами: шифрование электронной  
 почты, электронной подписи, интел­лектуальные банковские карточки и др  
 Естественно, что при этом основной вопрос для пользователя – обеспечивает ли  
 данное криптографическое сред­ство надежную защиту Но даже правильно  
 сформулировать этот элементар­ный вопрос непросто От какого противника  
 защищаемся? Какие возможно­сти у этого противника? Какие цели он может  
 преследовать? Как измерять надежность защиты? Список таких вопросов можно продолжить  
   
  Для  
 ответа на них пользователю необходимы знания основных понятий криптографии Для  
 ответа на них пользователю необходимы знания основных понятий криптографии  
 Цель данного раздела дать представление об  основных понятиях современной крип­тографии:  
 шифр, ключ, стойкость, электронная цифровая подпись, крипто­графический протокол  
 и др   
   
 Как  
 передать нужную информацию нужному адресату в тайне от других?   
   
 Размышляя  
 над задачей передачи конфиденциальных сведений, нетрудно прийти к выводу, что  
 для этого есть три возможности  
   
 1         
 Создать абсолютно надежный, недоступный для других канал  
 связи между абонентами

25 Классификация шифров

Классификация шифровСтойкость шифров ограниченного использования основывается на сохранении в секрете алгоритма криптографического преобразования в силу его уязвимости, малого количества ключей или отсутствия таковых (секретные кодовые системы)Стойкость шифров общего использования основывается на секретности ключа и сложности его подбора потенциальным противникомII По особенностям алгоритма шифрования шифры общего использования можно разделить на следующие видыВ одноключевых системах для шифрования и дешифрования используется один и тот же ключВ аддитивных шифрах буквы алфавита заменяются числами, к которым затем добавляются числа секретной случайной (псевдослучайной) числовой последовательности (гаммы), после чего берется остаток от деления по модулю (операция mod) Если исходное сообщение и гамма представляются в битовом виде, то при шифровании и расшифровании применяется логическая операция «Исключающее ИЛИ» (XOR, сложение по модулю 2)Квантовая криптография вносит в процесс шифрования естественную неопределенность квантового мира Процесс отправки и приёма информации выполняется посредством объектов квантовой механики (например, при помощи электронов в электрическом токе или фотонов в линиях волоконно-оптической связи) Самым ценным свойством этого вида шифрования является то, что при посылке сообщения отправляющая и принимающая сторона с достаточно большой вероятностью могут установить факт перехвата противником зашифрованного сообщенияВ двухключевых системах для шифрования и дешифрования используется два совершено разных ключа В детерминированных шифрах при шифровании одного и того же сообщения одним и тем же ключом всегда будет получаться один и тот же шифртекстКомбинированные (составные) методы предполагают использование для шифрования сообщения сразу нескольких методов (например, сначала замена символов, а затем их перестановка)III По количеству символов сообщения (или его кодовой замены), шифруемых или расшифровываемых по однотипной процедуре преобразования различают:

26 Подходы к построению криптосистем

В настоящем пособии изложены математические элементы теории чисел и теории поля, лежащие в основе построения современных криптографических систем, а также вопросы синтеза и анализа криптоалгоритмов Пособие предназначено для изучения лекционного курса "Математические основы криптологии" студентами специальностей 075400, 075300, 075600 Подготовлено на кафедре безопасности информационных технологий ТРТУЗавеса секретности вокруг этих технологий привела даже к тому, что в США криптографические алгоритмы были приравнены к вооружению, был введен запрет на вывоз шифровальных аппаратных и программных средств Затем были введены экспортные ограничения на длину используемого ключа в алгоритмах шифрования за пределами США, что позволяло американским спецслужбам производить дешифрацию сообщений на имеющихся вычислительных мощностях без знания укороченного ключа С 1 марта 2001 г экспортные ограничения были сняты Из-за событий, произошедших 11 сентября того же года, наблюдается ужесточение государственного контроляПостоянно возрастающие вычислительные мощности заставляли использовать все более сложные алгоритмы криптопреобразования или увеличивать длину ключей, используемых при шифрованииСтандарты на криптографические алгоритмы устаревали, становились ненадежными Информация, закрытая на некотором ключе, уже не могла храниться конфиденциально достаточно долго - столько, сколько полагалось по государственным нормамНо даже такой размер ключа позволял решить проблему вскрытия шифра объединенным группам за дни и даже за часы параллельной работы В дальнейшем потребовался переход на ключи, которые в несколько раз длиннее упомянутых Но и это была только временная мера, и недавно были приняты новые стандарты на алгоритмы криптопреобразований (AES в США)Симметричные алгоритмы шифрованияПрактика показала, что чем больше известен алгоритм, чем больше людей работало с ним, тем более проверенным, а значит, и надежным он становится Так, публично известные алгоритмы сейчас выдерживают борьбу со временем, а вот засекреченные государственные шифры обнаруживают в себе множество ошибок и недочетов, т к всего учесть невозможно

27 Криптографическая стойкость шифров

Криптографическая стойкость (или криптостойкость) — способность криптографического алгоритма противостоять криптоанализу Рассмотрим условия, которым должна удовлетворять криптосистема для надежной защиты информации Стойкость зашифрованной информации (криптографическая стойкость, или просто стойкость) зависит от возможности несанкционированного чтения данных Практическая стойкость таких систем базируется на теории сложности и оценивается исключительно в расчёте на определённый момент времени и последовательно c двух позиций: Дальнейшее исследование алгоритма с целью поиска слабостей (уязвимостей) (криптоанализ) добавляет оценки стойкости по отношению к известным криптографическим атакам (линейный, дифференциальный криптоанализ и др) и могут понизить известную стойкость Например, для многих симметричных шифров существуют слабые ключи[en] и S-блоки, применение которых снижает криптографическую стойкость Чем более длительным и экспертным является анализ алгоритма и реализаций, тем более достоверной можно считать его стойкость В нескольких случаях длительный и внимательный анализ приводил к снижению оценки стойкости ниже приемлемого уровня (например, в черновых версиях FEAL) Криптографическая стойкость (или криптостойкость) — способность криптографического алгоритма противостоять криптоанализу Стойким считается алгоритм, который для успешной атаки требует от противника недостижимых вычислительных ресурсов, недостижимого объёма перехваченных открытых и зашифрованных сообщений или же такого времени раскрытия, что по его истечению защищенная информация будет уже не актуальна, и т д В большинстве случаев криптостойкость нельзя математически доказать, можно только доказать уязвимости криптографического алгоритмаВ основном применяются практически стойкие или вычислительно стойкие системы Стойкость этих систем зависит от того, какими вычислительными возможностями обладает криптоаналитик Практическая стойкость таких систем базируется на теории сложности и оценивается исключительно на какой-то определенный момент времени и последовательно c двух позиций:

28 Принципы построения и функционирования блочных шифров

Единицей кодирования при использовании блочных шифров является блок, состоящий из нескольких байтов (от 4 до 32) Результат кодирования зависит от всех исходных байтов этого блока Схема применяется при пакетной передаче информации и кодировании файловВыделяют два общих принципа построения шифров: рассеиваниеи перемешиваниеПеремешиванием называется использование таких шифрующих преобразований, которые усложняют восстановление взаимосвязи символов открытого и зашифрованного текста, а также ключа и зашифрованного текстаСеть Фейстеля(Horst Feistel 1915-1990 гг)Большинство современных блочных шифров используют сетьАбсолютная стойкость криптосистемы обуславливается отсутствием всяких закономерностей в зашифрованных данных В этом случае становится невозможно получить какую-либо информацию об исходном тексте Это достигается при выполнении следующих требований: равенство длин ключа и исходного текста; случайность ключа; однократное использование ключаОбщие сведения о блочных шифрахХарактерной особенностью блочных криптоалгоритмов является тот факт, что в ходе своей работы они производят преобразование блока входной информации…Основные принципы построения службыСБШ используют в различных режимах шифрования, построенных на основе базового режима, реализующего множество подстановок большой степени Базовый режим называется электронной кодовой книгой (англ — ЕСВ) или простой заменой Блочный шифр в режиме ЕСВ моделируется автоматом ЛЕСВ = (X, Y, К, /) без памяти (5 = 0), где X = Y = V2„ и функция выходов f(x, k) биективна по входной переменной х Уравнения шифрования при ключе k е К имеют вид  
 Подстановки Ek построены по итеративному принципу Пусть ф(х, q) (8(х, q), я(х, q)) — биективное по переменной х отображение ^ х Q V2„(V2n xQ'^ V2rl), где х е V2,„ q е Q (q е Q') и Q (Q') - множество производных ключей, генерируемых из основного ключа к При построении подстановки Ек используются производные ключи <у(), qr+{ из (У и где {0О, 0,,где х — блок открытого текста Алгоритм расшифрования реализует подстановку Ек1 для блока шифротекста у Из равенства (153) получаем

29 Симметричные криптоалгоритмы

Симметричные криптографические алгоритмы шифрования(Симметричные\_криптосистемы) - способ шифрования, в котором для шифрования и расшифрования применяется один и тот же криптографический ключ Ключ алгоритма должен сохраняться в секрете обеими сторонамиКлассическим примером таких алгоритмов являются симметричные криптографические алгоритмы, перечисленные ниже:Симметричные криптосистемы — (также симметричное шифрование, симметричные шифры)  способ шифрования, в котором для шифрования и расшифровывания применяется один и тот же криптографический ключ До изобретения схемы асимметричного шифрования единственным существовавшим… …   ВикипедияКриптопровайдер — (Cryptography Service Provider, CSP)  это независимый модуль, позволяющий осуществлять криптографические операции в операционных системах Microsoft, управление которым происходит с помощью функций CryptoAPI Проще говоря, это посредник между …   ВикипедияИнтегральный криптоанализ — метод криптоанализа, объединяющий ряд атак на симметричные блочные криптографические алгоритмы В отличие от дифференциального криптоанализа, который рассматривает воздействие алгоритма на пару открытых текстов, интегральный криптоанализ… …   ВикипедияБыстрая криптосистема с открытым ключом — (англ Fast public key cryptosystem) или лёгкая криптосистема с открытым ключом (англ Lightweight public key cryptosystem)  асимметричная криптосистема, используемая в устройствах с ограниченными ресурсами Обычные криптографические алгоритмы… …   ВикипедияСимметричное шифрование — это способ шифрования данных, при котором один и тот же ключ используется и для кодирования, и для восстановления информации До 1970-х годов, когда появились первые асимметричные шифры, оно было единственным криптографическим методом Как правило, биты исходных данных сравниваются с битами секретной последовательности с помощью логической операции XOR (исключающее ИЛИ, на выходе дающее 0, если значения битов совпадают, и 1, если они различаются)Потоковое шифрование в настоящее время используют следующие алгоритмы:

30 Принципы построения и функционирования поточных шифров

Цель лекции: познакомиться с понятием "поточный шифр", а также с принципами использования генераторов псевдослучайных ключей при потоковом шифрованииСовременная информатика широко использует псевдослучайные числа в самых разных приложениях — от методов математической статистики и имитационного моделирования до криптографии При этом от качества используемых генераторов псевдослучайных чисел (ГПСЧ) напрямую зависит качество получаемых результатовГПСЧ могут использоваться в качестве генераторов ключей в поточных шифрах Целью использования генераторов псевдослучайных чисел является получение "бесконечного" ключевого слова, располагая относительно малой длиной самого ключа Генератор псевдослучайных чисел создает последовательность битов, похожую на случайную На самом деле, конечно же, такие последовательности вычисляются по определенным правилам и не являются случайными, поэтому они могут быть абсолютно точно воспроизведены как на передающей, так и на принимающей стороне Последовательность ключевых символов, использующаяся при шифровании, должна быть не только достаточно длиннойДля использования в криптографических целях генератор псевдослучайных чисел должен обладать следующими свойствами:При наличии указанных свойств последовательности псевдослучайных чисел могут быть использованы в поточных шифрах В силу ряда естественных причин, связанных с простотой реализации и необходимостью достижения высоких скоростей шифрования, наибольшее распространение получили шифры, осуществляющие побуквенное зашифрование с помощью некоторого множества подстановочных преобразований алфавита открытых сообщений Другими словами, речь идет об эндоморфных поточных многоалфавитных шифрах замены с множествами шифрвеличин и шифробозначений, совпадающими с алфавитом открытых сообщений Далее рассматриваемые поточные шифры мы будем предполагать именно такимиПоточный шифр — это симметричный шифр, в котором каждый символ открытого текста преобразуется в символ шифрованного текста в зависимости не только от используемого ключа, но и от его расположения в потоке открытого текста Поточный шифр реализует другой подход к симметричному шифрованию, нежели блочные шифры

31 Принципы построения криптоалгоритмов с открытым ключом

Для генерации ЭП и для расшифровки сообщения используется закрытый ключ[1] Криптографические системы с открытым ключом в настоящее время широко применяются в различных сетевых протоколах, в частности, в протоколах TLS и его предшественнике SSL (лежащих в основе HTTPS), в SSH Также используется в PGP, S/MIME Асимметричное шифрование с открытым ключом базируется на следующих принципах: Если необходимо передать зашифрованное сообщение владельцу ключей, то отправитель должен получить открытый ключ Отправитель шифрует свое сообщение открытым ключом получателя и передает его получателю (владельцу ключей) по открытым каналам При этом расшифровать сообщение не может никто, кроме владельца закрытого ключа Этот принцип можно объяснить через бытовую аналогию «замо́к — ключ от замка́» для отправки посылки У участника A есть личный замок и ключ от него Если участник А хочет получить секретную посылку от участника Б, то он публично передаёт ему свой замок Участник Б защёлкивает замок на секретной посылке и отправляет её участнику А Получив посылку, участник А открывает ключом замок и получает посылку Но сама односторонняя функция бесполезна в применении: ею можно зашифровать сообщение, но расшифровать нельзя Поэтому криптография с открытым ключом использует односторонние функции с лазейкой Лазейка — это некий секрет, который помогает расшифровать То есть существует такой y {\displaystyle y} , что, зная f ( x ) {\displaystyle f(x)} и y {\displaystyle y} , можно вычислить x {\displaystyle x} Например, если разобрать часы на множество составных частей, то очень сложно собрать вновь работающие часыПонять идеи и методы криптографии с открытым ключом помогает следующий пример — хранение паролей в удалённом компьютере, к которому должны подключаться пользователи Каждый пользователь в сети имеет свой пароль При входе он указывает имя и вводит секретный пароль Но если хранить пароль на диске удалённого компьютера, то кто-нибудь его может считать (особенно легко это сделать администратору этого компьютера) и получить доступ к секретной информации Для решения задачи используется односторонняя функция

32 Современные криптоалгоритмы с открытым ключом

Для генерации ЭП и для расшифровки сообщения используется закрытый ключ[1] Криптографические системы с открытым ключом в настоящее время широко применяются в различных сетевых протоколах, в частности, в протоколах TLS и его предшественнике SSL (лежащих в основе HTTPS), в SSH Также используется в PGP, S/MIME Асимметричное шифрование с открытым ключом базируется на следующих принципах: Если необходимо передать зашифрованное сообщение владельцу ключей, то отправитель должен получить открытый ключ Отправитель шифрует свое сообщение открытым ключом получателя и передает его получателю (владельцу ключей) по открытым каналам При этом расшифровать сообщение не может никто, кроме владельца закрытого ключа Этот принцип можно объяснить через бытовую аналогию «замо́к — ключ от замка́» для отправки посылки У участника A есть личный замок и ключ от него Если участник А хочет получить секретную посылку от участника Б, то он публично передаёт ему свой замок Участник Б защёлкивает замок на секретной посылке и отправляет её участнику А Получив посылку, участник А открывает ключом замок и получает посылку Но сама односторонняя функция бесполезна в применении: ею можно зашифровать сообщение, но расшифровать нельзя Поэтому криптография с открытым ключом использует односторонние функции с лазейкой Лазейка — это некий секрет, который помогает расшифровать То есть существует такой y {\displaystyle y} , что, зная f ( x ) {\displaystyle f(x)} и y {\displaystyle y} , можно вычислить x {\displaystyle x} Например, если разобрать часы на множество составных частей, то очень сложно собрать вновь работающие часыПонять идеи и методы криптографии с открытым ключом помогает следующий пример — хранение паролей в удалённом компьютере, к которому должны подключаться пользователи Каждый пользователь в сети имеет свой пароль При входе он указывает имя и вводит секретный пароль Но если хранить пароль на диске удалённого компьютера, то кто-нибудь его может считать (особенно легко это сделать администратору этого компьютера) и получить доступ к секретной информации Для решения задачи используется односторонняя функция

33 Имитостойкость и помехоустойчивость шифров

Любой шифр, нс размножающий искажений типа «замена» символов в шиф- ротексте, представим в виде композиции шифров многозначной замены и перестановки (теорема А А Маркова) Всякий шифр, не размножающий искажений типа «пропуск» символов в шифротексте, есть либо шифр простой замены, либо произведение шифра простой замены и частного вида шифра перестановки, заключающегося в инверсии записи текста (запись справа налево)Имитозащита — это защита канала шифрованной связи от навязывания ложной информации Ложная информация считается навязанной, если она принята приемным устройством к исполнению, те таким же образом, как принимаются истинные сообщенияПредположим, что имеется связь между абонентами А и В Абонент А может в определенный момент времени отправить абоненту В криптограмму До момента передачи криптограммы канал «пуст», но в шифратор або- нента-получателя В введен ключ шифрования в ожидании получения сообщения от абонента-отправителя АИмитация при «пустом» канале Пусть канал связи «пуст» и противник вставляет в канат связи некоторое шифрованное сообщение Возможны два исхода:Для обеспечения имитозащиты используется криптографическая контрольная сумма, зависящая от открытого текста и ключа — имитовставка алгоритма ГОСТ или код аутентификации (MAC — Message Authentication Code) зарубежных алгоритмов шифрования Кроме того, криптографически стойкими являются некоторые алгоритмы вычисления хэш-значения (контрольной суммы), построенные на односторонних функциях Защита от переадресации и изменения отправителя достигается использованием технологии ЭЦП-Для многих симметричных шифров существуют слабые ключи и 5-блоки, применение которых снижает криптографическую стойкость Также важным способом проверки стойкости являются атаки на реализацию, выполняемые для конкретного программно-аппаратно-человеческого комплексаВ той или иной мере этим требованиям отвечают:При решении проблемы имитостойкости противник может не только видеть все криптограммы, передаваемые по каналу, но способен также изменять их по своему желанию Законный получатель защищает себя от обмана, дешифрируя все полученные сообщения и принимая только те, которые зашифрованы правильным ключом

34 Универсальные методы криптоанализа

Криптоанализом (от греческого krypts - "скрытый" и analein - "ослаблять" или избавлять") называют науку восстановления (дешифрования) открытого текста без доступа к ключу Хотя история криптоанализа насчитывает многие века, особенно интенсивно эта область знаний начала развиваться с наступлением компьютерной эрыВеликий сыщик Шерлок Холмс утверждал, что "любая тайна, порожденная человеческим сознанием, им же может быть и раскрыта" Его слова были в середине 40х гг прошлого века опровергнуты великим ученым и основоположником современной криптографии Клодом Шенноном Он показал ([65]), что если на любой исходный текст наложить (тПопытка криптоанализа называется атакой Криптоанализ ставит своей задачей в разных условиях получить дополнительные сведения о ключе шифрования, чтобы значительно уменьшить диапазон вероятных ключей Результаты криптоанализа могут варьироваться по степени практической применимости Так, криптограф Ларс Кнудсен [67] предлагает следующую классификацию успешных исходов криптоанализа блочных шифров в зависимости от объема и качества секретной информации, которую удалось получить:Появление новых криптографических алгоритмов приводит к разработке методов их взлома Если целью криптоаналитика является раскрытие возможно большего числа шифров (независимо от того, хочет ли он этим нанести ущерб обществу, предупредить его о возможной опасности или просто получить известность), то для него наилучшей стратегией является разработка универсальных методов анализа [61] Но эта задача является также и наиболее сложной Результатом возникновения каждого нового метода криптоанализа является пересмотр оценок безопасности шифров, что, в свою очередь, влечет необходимость создания более стойких шифровНа рис61 методы криптоанализа систематизированы по хронологии их появления и применимости для взлома различных категорий криптосистем На вертикальной оси обозначены области применения методов криптоанализа: для взлома криптосистем с секретным ключом, открытым ключом или хеш-функций

35 Криптоанализ симметричных алгоритмов

Рассматриваются основные аспекты применения современных методов криптоанализа для оценки стойкости симметричных блочных алгоритмов шифрования В том числе, рассмотрены такие методы анализа как линейный, дифференциальный, алгебраический анализы, слайдовая атака Также рассмотрены различные подходы к анализу стандарта AES Дано определение Парадоксу дней рождений и объяснена его роль в решении задач защиты информации При рассмотрении подходов к анализу современных симметричных криптосистем отдельное внимание уделено вопросам возможности применения распределенных многопроцессорных вычислений с целью сокращения времени анализаРассматриваются основные аспекты применения современных методов криптоанализа для оценки стойкости симметричных блочных алгоритмов шифрования В том числе, рассмотрены такие методы анализа как линейный, дифференциальный, алгебраический анализы, слайдовая атака Также рассмотрены различные подходы к анализу стандарта AES Дано определение Парадоксу дней рождений и объяснена его роль в решении задач защиты информации При рассмотрении подходов к анализу современных симметричных криптосистем отдельное внимание уделено вопросам возможности применения распределенных многопроцессорных вычислений с целью сокращения времени анализакриптоанализа, который аналитик сможет использовать Рассмотрим основные виды криптоанализа современных симметричных криптосистем3 Анализ правильных пар текстов и накопление статистики о возможных значениях секретного ключа шифрованияВторой шаг анализа является вычислительно стойкой задачей для любого алгоритма шифрования, при этом не важно, обладает он фиксированными или нефиксированными элементами Анализ заключается в опробовании большого числа пар текстов с целью определения являются ли они правильной парой текстов, то есть той парой текстов, которую в дальнейшем можно использовать для анализа с целью поиска секретного ключа шифрования Данный шаг может и должен быть легко представим в виде параллельных вычислений для сокращения времени анализа

36 Криптоанализ асимметричных алгоритмов

по теме: «Криптоанализ асимметричных шифров» 1 Глава 2 Методы криптоанализа асимметричных криптосистем 13 21Криптоанализ систем шифрования, основанных на сложности задачи дискретного логарифмирования 13 22Криптоанализ систем шифрования, основанных на сложности задачи факторизации 16 Кардинальное отличие криптосистемы с открытым ключом (по другой терминологии, несимметричной системы) от симметричной системы состоит в том, что в криптосистемах с открытым ключом процедура зашифровывания становится общедоступной Это, однако, не означает как в традиционных системах шифрования, что общедоступной является и процедура расшифровывания Понятие ключа разбивается на две части (включает теперь два понятия): ключ открытый, и ключ секретный Общедоступный открытый ключ используется для зашифровывания, но расшифровывание может осуществить только тот, кто владеет секретным ключом Именно как раз в допущении того, что нахождение ключа расшифровывания по известному ключу зашифровывания может быть сложно-вычислимой задачей, и заключается идея, которая определила дальнейшее направление развития криптографии Но наравне с криптографией шло развитие и криптоанализа – другого противоположного раздела криптологии, предметом которого является разработка методов взлома новых криптографических алгоритмов с целью выявления их надежности Результатом возникновения каждого нового метода криптоанализа является пересмотр оценок безопасности шифров, что в свою очередь, влечет необходимость создания более стойких шифров Целью курсовой работы является анализ надежности алгоритмов ассиметричных методов шифрования Во второй главе будут описаны методы криптоанализа, основанные на особенностях систем шифрования с открытым ключом Криптографическая система с открытым ключом – система шифрования, при которой открытый ключ передаётся по открытому каналу связи, и используется для шифрования сообщения, а для расшифрования сообщения используется секретный ключ Но сама односторонняя функция бесполезна в применении: ею можно зашифровать сообщение, но расшифровать нельзя Поэтому криптография с открытым ключом использует односторонние функции с лазейкой Лазейка — это некий секрет, который помогает расшифровать То есть существует такой y, что зная f(x), можно вычислить x К примеру, если разобрать часы на множество составных частей, то очень сложно собрать вновь работающие часы

37 Криптографические хэш-функции

Имея заданное значение h, должно быть сложно найти любое сообщение m такое, что Имея заданное входное значение , должно быть сложно найти другое входное значение такое, чтоSecond pre-image resistance Это свойство называют сопротивлением второму прообразу Для упрощения можно сказать, что это свойство находится где-то посередине между двумя предыдущими Атака по нахождению второго прообраза происходит, когда злоумышленник находит определенный вход, который генерирует тот же хеш, что и другой вход, который ему уже известен Другими словами, злоумышленник, зная, что пытается найти такое, что В данной статье я постарался объяснить, что такое хеш-функция и зачем она нужнаТакже в общих чертах мной был разобран принцип работы алгоритма SHA-3 Keccak, который является последним стандартизированным алгоритмом семейства Secure Hash AlgorithmКриптографическая хеш-функция является доказуемо защищённой от коллизий, если задача нахождения коллизий может быть средуцирована за полиномиальное время[en] от задачи P {\displaystyle P} , которая считается неразрешимой за полиномиальное время Криптографические хеш-функции широко используются в практике защиты информации, такой как цифровые подписи, коды аутентификации сообщений и другие формы аутентификации Криптографические хеш-функции должны иметь следующие свойства (источник: википедия):1 Одно и то же сообщение всегда приводит к одному и тому же хеш-значению (теSHA-1 (безопасный алгоритм хеширования 1) - это криптографическая хеш-функция, которая может преобразовывать произвольно длинную строку данных в дайджест с фиксированным размером 160 бит Этот дайджест обычно отображается в виде шестнадцатеричного числа из 40 символовАлгоритм SHA-1 теперь считается небезопасным, Сертификаты SHA-1 больше не соответствуют базовым требованиям форума CA / B или поддерживаются текущими версиями основных веб-браузеровСерия хэш-функций алгоритма безопасного хеширования (SHA) состоит из различных наборов (SHA-0, SHA-1, SHA-2, SHA-3)Хеш функция Дженкинса — Криптографическая хеш функция Название Хэш функции Дженкинса Впервые опубликован 1997 Тип хеш функция Хэш функции Дженкинса представляют собой семейство хэш функций общего назначения для ключей переменной длины разработанных Бобом Дженкинсом… …   Википедия

38 Электронная подпись

Поможем получить и установить подпись  
 ФНС Расскажем, как работать на Госуслугах, в ЕГАИС, системе маркировки и др  
 Разрешим сложности в торгах и прикрепим подпись на ЭТПМы сами приедем к вам, чтобы удостоверить личность, забрать документы  
 и выдать токен После этого вы сможете выпустить  
 подпись на своём компьютереПолучите электронную подпись, не приезжая к нам в офис Это возможно,  
 если у вас есть действующая подпись другого УЦРаботаем на рынке давно Подбираем подпись под ваши задачиЭлектронная подпись (ранее ЭЦП) — собственноручная подпись в электронном виде, которой можно подписывать документы Федеральный закон №63‑ФЗ от 06042011 определил три вида электронных подписей: простую, неквалифицированную и квалифицированную У них разный уровень защиты и юридической значимости, так что применяются они в разных ситуацияхПростая ЭП — это логин/пароль или код из СМС, которые вы вводите для авторизации в интернет‑магазине, портале «Госуслуги» или внутренней корпоративной сети, подтверждая свою личность Простая электронная подпись имеет юридическую силу при оказании страховых, государственных и муниципальных услуг, а также если участники документооборота договорятся о ее признанииСамая защищенная подпись, обладающая теми же возможностями, что и неквалифицированная В отличие от нее, квалифицированная подпись создается с использованием средств шифрования, сертифицированных ФСБ Выдается квалифицированная ЭП только в удостоверяющих центрах, аккредитованных Минкомсвязи России Любой документ, который законом не запрещено оформлять в электронном виде, можно подписывать квалифицированной электронной подписью Он будет иметь полную юридическую силуЧтобы узнать, какая именно, позвоните в техподдержку удостоверяющего центра Если вы получали подпись в УЦ «Тензор», сообщите специалисту техподдержки ваш ИНН и он подскажет тип ЭППростая электронная подпись подойдет любым физическим лицам, которые пользуются интернет‑сервисами для покупок товаров и услуг, управления средствами в банке Может использоваться для оплаты штрафов ГИБДД и получения некоторых услуг на портале «Госуслуги»

39 Управление криптографическими ключами

Управление ключами состоит из процедур, обеспечивающих: Управление ключами играет важнейшую роль в криптографии как основа для обеспечения конфиденциальности обмена информацией, идентификации и целостности данных В случае использования ключей для обеспечения безопасности хранимой информации субъектом может быть единственный пользователь, который осуществляет работу с данными в последовательные промежутки времени Управление ключами в сетях связи включает, по крайней мере, двух субъектов — отправителя и получателя сообщения Целью управления ключами является нейтрализация таких угроз, как: Управление ключами обычно осуществляется в контексте определенной политики безопасности Политика безопасности прямо или косвенно определяет те угрозы, которым должна противостоять система Кроме того, она определяет: Одной из важных характеристик системы управления ключами являются сроки действия ключей Срок действия ключа означает промежуток времени, в течение которого он может быть использован доверенными сторонами В жизненном цикле управления ключами важную роль играет так называемая доверенная третья сторона Согласно определению, данному в Рекомендации ITU T серия X842, ДТС — это организация или её агент, предоставляющий один или более сервисов в области безопасности, которому доверяют другие объекты как поставщику данных услуг Основными категориями служб ДТС являются: 7 Управление  криптографическими ключами         Управление ключами – информационный процесс, включающий реализацию следующих основных функций:         Генерация ключей для асимметричных криптосистем с открытыми ключами много сложнее, потому что эти ключи должны обладать определенными математическими свойствами (они должны быть очень большими и простыми и тд)            Очень важным условием безопасности информации является периодическое обновление ключевой информации в сети При этом должны переназначаться как рабочие ключи, так и мастер-ключи В особо ответственных сетях обновление ключевой информации (сеансовых ключей) желательно делать ежедневно Вопрос обновления ключевой информации тесно связан с третьим элементом управления ключами – распределением ключей

40 Реализации криптографических алгоритмов: программная, аппаратная, программно-аппаратная

На практике криптографические алгоритмы в зависимости от области применения имеют несколько типов реализации: программную, аппаратную и программно-аппаратную Перед тем как перейти непосредственно к рассмотрению достоинств и недостатков перечисленных типов реализации, сформулируем общие требования к реализации криптографических алгоритмов Современные алгоритмы шифрования должны удовлетворять следующим условиям:Аппаратная реализацияДо недавних пор алгоритмы шифрования реализовывались в виде отдельных устройств, что обусловливалось использованием криптографии для засекречивания различных видов передачи информации (телеграф, телефон, радиосвязь) С развитием средств вычислительной техники и общедоступных сетей передачи данных появились новые возможности применения криптографических алгоритмов Однако аппаратная реализация до сих пор широко используется не только в военной сфере, но и в коммерческих организациях Подобная «живучесть» аппаратных средств криптографической защиты информации объясняется рядом факторовВо-первых, аппаратная реализация обладает лучшими скоростными характеристиками, нежели программно реализуемые алгоритмы шифрования Использование специальных чипов, адаптированных к реализации на них процедур зашифрования и расшифрования, приводит к тому, что, в отличие от процессоров общего назначения, они позволяют оптимизировать многие математические операции, применяемые в алгоритмах шифрованияПрограммная реализацияК недостаткам программных средств криптографической защиты следует отнести возможность вмешательства в действие алгоритмов шифрования и получения доступа к ключевой информации, хранящейся в общедоступной памяти Эти операции обычно выполняются при помощи простого набора программных инструментариев (отладчики программ и тд) Так, например, во многих операционных системах осуществляется аварийный дамп памяти на жесткий диск, при этом в памяти могут находиться ключи, найти которые не составит трудаТаким образом, слабая физическая защищенность программных средств является одним из основных недостатков подобных методов реализации алгоритмов шифрования

41 Композиция криптографических методов в систему защиты информации

Данный учебник знакомит с основными принципами, подходами и методами современной криптографии Наряду с историческими шифрами рассмотрены используемые в настоящее время криптосистемы с секретными и открытыми ключами, криптографические хэш-функции, методы электронной подписи, криптосистемы на эллиптических кривых Освещены вопросы применения криптографических методов и средств защиты информации для обеспечения конфиденциальности, подтверждения целостности, аутентификации и решения других практических задач в современных информационных системах По окончании курса Вы получите печатное удостоверение о повышении квалификации установленного образца (доставка удостоверения бесплатна) Криптографические методы защиты информацииКлассификация криптографических методов защиты информации 4Одна из основных проблем такого развития является проблема защиты передаваемой и получаемой информации На любом из этапов передачи электронной информации от отправителя до получателя существует множество возможных видов атак на систему обмена и хранения информации, можно сделать вывод о том, что основным понятием в системе обмена электронной информацией является аутентификация Один из способов решения этой проблемы, применение криптографической защиты информации[1]Проблемы защиты конфиденциальности и целостности информации тесно связаны между собой, поэтому методы решения одной из них часто применимы для решения другойИзвестны различные подходы к классификации методов криптографического преобразования информации По виду воздействия на исходную информацию методы криптографического преобразования информации могут быть разделены на четыре группы:В отличие от других методов криптографического преобразования информации, методы стеганографии позволяют скрыть не только смысл хранящейся или передаваемой информации, но и сам факт хранения или передачи закрытой информации В основе всех методов стеганографии лежит маскирование закрытой информации среди открытых файлов, те скрываются секретные данные, при этом создаются реалистичные данные, которые невозможно отличить от настоящих Обработка мультимедийных файлов в информационных системах открыла практически неограниченные возможности перед стеганографией

42 Криптографические стандарты

Есть множество стандартов, относящихся к криптографии Стандартов защиты информации – много  
 Некоторые из этих стандартов касаются практически любой IT-системы, не являясь жёстко “отраслевыми”, поэтому работающему с security-решениями нужно хотя бы рамочно ориентироваться в оных  
 Данная статья – краткая выжимка из рассказываемого на курсе Microsoft 2821B, поэтому может рассматриваться как допматериал для тех, кто нуждается в более глубоких знаниях, чем дающихся на ознакомительных и базовых курсах уровня MCSE / CCIE:SecurityНекоторые из этих стандартов касаются практически любой IT-системы, не являясь жёстко “отраслевыми”, поэтому работающему с security-решениями нужно хотя бы рамочно ориентироваться в оных  
 Данная статья – краткая выжимка из рассказываемого на курсе Microsoft 2821B, поэтому может рассматриваться как допматериал для тех, кто нуждается в более глубоких знаниях, чем дающихся на ознакомительных и базовых курсах уровня MCSE / CCIE:Security  
 FIPS 140-1 и FIPS 140-2 FIPS – это Federal Information Processing Standards, разрабатываемые для формализации требований к криптографической защите информации в госДанная статья – краткая выжимка из рассказываемого на курсе Microsoft 2821B, поэтому может рассматриваться как допматериал для тех, кто нуждается в более глубоких знаниях, чем дающихся на ознакомительных и базовых курсах уровня MCSE / CCIE:Security  
 FIPS 140-1 и FIPS 140-2 FIPS – это Federal Information Processing Standards, разрабатываемые для формализации требований к криптографической защите информации в госорганах СШАНачнём  
 FIPS 140-1 и FIPS 140-2 FIPS – это Federal Information Processing Standards, разрабатываемые для формализации требований к криптографической защите информации в госорганах США Чтобы какое-либо ПО или оборудование могло быть сертифицировано для использования в этих структурах – ну либо связанных с ними – должна быть возможность работы в “FIPS-режиме”  
 На данный момент существует 2 принятых версии стандартов FIPS – FIPS 140-1 (с января 1994 года) и FIPS 140-2 (с мая 2001 года) – и рассматриваемый с 2009 года FIPS 140-3

43 Криптографические протоколы

Криптографический протокол (англ Cryptographic protocol) — это абстрактный или конкретный протокол, включающий набор криптографических алгоритмов, часто являющихся последовательностью криптографических примитивов В основе протокола лежит набор правил, регламентирующих использование криптографических преобразований и алгоритмов в информационных процессах для обмена сообщениями между двумя и более участниками, а также описание используемых структур[⇨] В протоколе участниками (субъектом, стороной) могут быть приложения, люди, их группы или, например, организации Другими словами — всё, по каким-либо причинам способное иметь активную или пассивную роль в работе протокола Так, в частности, большинство протоколов разрабатывается с учётом наличия пассивного слушателя, способного перехватывать сообщения[⇨] Появление самых простых протоколов датируется концом 1970-х, началом 1980-х годов[1] Вклад в их появление внесли такие специалисты, как Рональд Ривест, Ади Шамир[2], Роджер Нидхем, Майкл Шрёдер[3] и многие другие Брюс Шнайер приводит описание известных протоколов в своей книге «Прикладная Криптография»[4] Криптографический протокол имеет следующие функции[5]: Протокол делится на проходы (англ pass) или циклы (англ round), являющиеся интервалом времени активности только одного участника В протоколах, рассчитанных на количество участников большее двух, при необходимости их синхронизации циклом называют период времени между двумя точками синхронизации[6] Реализация протокола или даже теоретическое её описание для конкретных участников, каждый из которых имеет одну или несколько ролей, называется сеансом (англ session) В другом сеансе протокола участники могут поменяться ролями и выполнять уже совсем другие функции[6] Таким образом, протокол описывает правила поведения каждой абстрактного участника в протоколе А сеанс описывает уже состоявшейся в прошлом конкретную реализацию протокола[6] При записи криптографических протоколов для обозначения участников принято использовать либо термины «отправитель», «получатель», пр, либо экземплификанты Соответствие между ними следующее[6]:

44 Информация как объект правового регулирования

Статья 4 Информация как объект правового регулирования1 Информация является объектом гражданских прав и может свободно использоваться и передаваться одним лицом другому, если федеральным законом не установлены ограничения на доступ к информации или требования к порядку ее распространения либо предоставленияСтатья 5 Информация как объект правовых отношений1 Информация может являться объектом публичных, гражданских и иных правовых отношений Информация может свободно использоваться любым лицом и передаваться одним лицом другому лицу, если федеральными законами не установлены ограничения доступа к информации либо иные требования к порядку ее предоставления или распространения2 Информация в зависимости от категории доступа к ней подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа)3 Информация в зависимости от порядка ее предоставления или распространения подразделяется на:  
   
 Директор по взаимодействию с органами государственной власти ПАО «Ростелеком» Ирина Сиренко в своем выступлении рассказала об условиях использования видеоизображения как объекта гражданских прав и как доказательства в судебной практике Во-первых, необходимо принять локальный нормативный акт, регулирующий порядок ведения видеонаблюдения, и ознакомить с данным актом всех сотрудников компании Видеонаблюдение допускается только для общественных интересов или при осуществлении лицом публичных функций (например, на концерте) и недопустимо в целях извлечения прибыли, если видеосъемка ведется, когда лицо не осуществляет публичных функций и находится в частном месте Ирина Сиренко обратила особое внимание, что основанием иска становится не видеонаблюдение, а обнародование снятого видео  
 Доцент кафедры гражданского права Уральского государственного юридического университета Дмитрий Мурзин в своем выступлении остановился на проблеме определения места информации в системе объектов гражданских прав Он отметил, что суды на сегодняшний день занимают позицию, согласно которой использовать информацию, размещенную гражданином, можно только с его согласия, поскольку она подпадает под охрану личных неимущественных прав

45 Законодательство РФ в области информационной безопасности

В России действуют законы, где описано, как правильно работать с информацией: кто отвечает за ее сохранность, как ее собирать, обрабатывать, хранить и распространять Стоит знать их, чтобы случайно что-нибудь не нарушитьМы собрали для вас пять основных ФЗ о защите информации и информационной безопасности и кратко рассказали их ключевые моменты149-ФЗ — главный закон об информации в России Он определяет ключевые термины, например, говорит, что информация — это любые данные, сведения и сообщения, представляемые в любой форме Также там описано, что такое сайт, электронное сообщение и поисковая система Именно на этот закон и эти определения нужно ссылаться при составлении документов по информационной безопасностиВ 149-ФЗ сказано, какая информация считается конфиденциальной, а какая — общедоступной, когда и как можно ограничивать доступ к информации, как происходит обмен данными Также именно здесь прописаны основные требования к защите информации и ответственность за нарушения при работе с нейЭтот закон регулирует работу с персональными данными — личными данными конкретных людей Его обязаны соблюдать те, кто собирает и хранит эти данные Например, компании, которые ведут базу клиентов или сотрудников Мы подробно рассматривали этот закон в отдельной статье «Как выполнить 152-ФЗ о защите персональных данных и что с вами будет, если его не соблюдать»Ключевые моменты закона о защите информации компании:Этот закон касается электронной подписи — цифрового аналога физической подписи, который помогает подтвердить подлинность информации и избежать ее искажения и подделки Закон определяет, что такое электронная подпись, какую юридическую силу она имеет и в каких сферах ее можно использовать Этот закон касается компаний, которые работают в сферах, критически важных для жизни государства — таких, что сбой в их работе отразится на здоровье, безопасности и комфорте граждан РоссииК таким сферам относится здравоохранение, наука, транспорт, связь, энергетика, банки, топливная промышленность, атомная энергетика, оборонная промышленность, ракетно-космическая промышленность, горнодобывающая промышленность, металлургическая промышленность и химическая промышленность Также сюда относят компании, которые обеспечивают работу предприятий из этих сфер, например, предоставляют оборудование в аренду или разрабатывают для них ПО

46 Правовой режим защиты коммерческой тайны

Согласно статистическим данным от ведущих аналитических компаний, частота и объемы утечек коммерческой информации растут с каждым годом При этом источником утечек далеко не всегда являются сторонние злоумышленники Зачастую причиной утечки информации становится ее доступность Наиболее подвержены угрозе утечки информации IT-компании, компании, занимающиеся высокими технологиямиКогда обнаруживается утечка ценной информации, пострадавшая сторона обращается в суд за защитой своих интересов Для защиты своих интересов и возмещения убытков, понесённых в следствии разглашения конфиденциальной информации требуется предоставить доказательства факта разглашения информации и наступления неблагоприятных последствий Чаще всего доказать последствия не представляется возможным в связи с отсутствием прямого ущерба нанесенного разглашением данных, и сложно прослеживаемой связью между утечкой данных и убытками компании Несомненно, информация, имеющая коммерческую значимость и ставшая известной третьим лицам, теряет свою ценность и влечет за собой потерю преимущества монопольного обладания, а также появление упущенной выгоды Такие последствия сложно доказуемы в суде любой юрисдикцииЮридически грамотная организация защиты конфиденциальной и ценной информации, корректное построение отношений, затрагивающих такую информацию, позволяет избежать вышеописанного сценария В условиях глобализации и информатизации деловых отношений, защита информации - первостепенная задача каждой компании В целях обеспечения защиты данных необходимо реализовать полный комплекс охранных мероприятийПравовой режим защиты коммерческой тайны - это основополагающий, законодательно закрепленный элемент защиты конфиденциальной коммерческой информацииКоммерческая тайна может включать в себя любую информацию, обладающую реальной или потенциальной экономической ценностью, в связи с неизвестностью ее сторонним лицам Для отнесения тех или иных данных к коммерческой тайне потребуется установление полноценного режима коммерческой тайны Правильно подобранный режим коммерческой тайны защищает и применяется к ноу хау, сведениям об организации рабочего процесса, базам клиентов, научно техническим разработках, маркетинговой стратегии, важным идеям и тд

47 Правовой режим защиты конфиденциальной информации

Правовой режим информации — нормативно установленные правила, определяющие степень открытости, порядок документирования, доступа, хранения, распространения и защиты информации, а также исключительные права на информацию[1] Основной целью введения правового режима информации является обеспечение информационной безопасности субъектов Статья описывает данное понятие в разрезе законодательства, применяемого в Российской Федерации Научно-технический прогресс характеризуется скачкообразным переходом к новейшим основам формирования производственного процесса Стадия формирования общества и связанных с ним технологий характеризуется соответствующими особенностями: формирование базовой науки и также ее соседних сфер, а также междисциплинарный и систематический подход к получению информации В этой связи развитие информационных правоотношений, их регулирование приобретает значение самостоятельной науки информационного права[2] Формирование государственной политики в сфере информации началось в 1999 г Впоследствии реализация государственной программы Российской Федерации «Информационное общество» (2011—2020), утвержденной постановлением Правительства РФ от 15 апреля 2014 г № 313, стала переходным моментом в истории построения российского информационного общества Целями указанной программы являлись повышение уровня жизни и улучшение качества работы граждан, улучшение условий работы организаций, формирование микроклимата для развития экономического потенциала страны на базе использования информационных и телекоммуникационных технологий[3] Правовое регулирование информации и тождественный ему правовой режим направлены на закрепление баланса общества и государства в постоянно меняющихся условиях формирования общественных, экономических, производственных и иных видов отношений Отдельное регулирование в сфере информации должно обеспечить своевременное в разрешение спорных ситуаций, связанных с реализацией права, а также сберечь механизм такой реализации для работы правовой системы в целом[4] В соответствии с указом Президента Российской Федерации от 7 мая 2018 г

48 Защита интеллектуальной собственности

В ст 1225 ГК РФ термином «интеллектуальная собственность» обозначаются результаты интеллектуальной деятельности субъекта и средства индивидуализации, которые снабжены правовой охраной, а также включены в исчерпывающий перечень, содержащийся в данной статьеОбъекты интеллектуальной собственности характеризуют следующие признаки:Важно! Защита права возможна только при условии подтверждения правообладателем собственных прав на объект Защита интеллектуальных прав стала предметом обзора судебной практики Президиума ВС РФ от 23092015 В частности, было отмечено такое усовершенствование системы защиты, как создание в 2013 году специализированного суда, назначением которого является повышение эффективности охраны указанных правЗащита интеллектуальной собственности должна строиться на четком разграничении способов защиты, установленных законодателем для разных категорий прав В определении ВС РФ от 23122014 № 5-КГ14-126 был сформулирован вывод о том, что правообладатель не может получить компенсацию морального вреда в случае нарушения исключительного права, поскольку этот способ имеет целью защиту прав только неимущественного характераЗащита интеллектуальной собственности в России не ограничивается гражданско-правовыми инструментами Нормы об ответственности за соответствующие нарушения есть в КоАП РФ, а также в УК РФИнтеллектуальная собственность согласно статье 138 Гражданского кодекса РФ являет собой исключительное право юридического лица или гражданина на результаты собственной интеллектуальной деятельности, а также на средства индивидуализации продукции и выполняемых услуг или работ Также под интеллектуальной собственностью подразумевают временное обладание смежными и авторскими правами, действующими патентами и свидетельствами на знаки обслуживания, товарные знаки, фирменные наименования Объектами интеллектуальной собственности являются неосязаемые, нематериальные объекты Интеллектуальной собственностью могут быть все без исключения результаты интеллектуальной деятельности в самых разнообразных сферах

49 Компьютерные правонарушения

Компьютерная преступность (преступление с использованием компьютера) — представляет собой любое незаконное, неэтичное или неразрешенное поведение, затрагивающее автоматизированную обработку данных или передачу данных При этом, компьютерная информация является предметом или средством совершения преступления Структура и динамика компьютерной преступности в разных странах существенно отличается друг от друга В юридическом понятии, компьютерных преступлений, как преступлений специфических не существует КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ, любое противоправное действие, при котором компьютер выступает либо как объект, против которого совершается преступление, либо как инструмент, используемый для совершения преступных действий Поскольку компьютерные системы получают все более широкое распространение, а деловые круги во все большей степени полагаются на компьютеры и часто хранят на них конфиденциальную информацию, преступники находят все больше путей использования компьютеров для совершения противоправных действий1 Одной из наиболее актуальных проблем правовой охраны компьютерной информации является определение понятия "компьютерное преступление" Общепринятого определения в науке уголовного права еще не предложено При этом, следует отметить, что его отсутствие является не только теоретической проблемой, оно также значительно усложняет деятельность правоохранительных органов по противодействию преступлениям в сфере использования компьютерной техникиТак, проведенный автором анализ отчетов УМВД в различных областях Украины свидетельствует о том, что достаточно часто к компьютерным преступлениям относят простые кражи компьютерной техники и изготовление поддельных документов с использованием компьютерной техники Понятно, что в таких условиях (даже, если не учитывать факторов технической оснащенности и наличия сотрудников со специальным образованием) эффективность борьбы правоохранительных органов с рассматриваемыми преступлениями значительно уменьшается2Вывод может быть только один: модификация средств и способов совершения преступления, использование с этой целью достижений научно-технического прогресса не изменяет тех отношений, на которые оно посягает, следовательно, не может влиять на квалификацию

50 Международное законодательство в области защиты информации

Законодательный уровень информационной безопасности можно разделитьЗаконодательный уровень является важнейшим для обеспечения информационной безопасности На этом уровне можно выделить следующие меры : Развитие средств, методов и форм автоматизации процессов хранения и обработки информации и массовое применение персональных компьютеров делают информацию гораздо более уязвимой Информация, циркулирующая в них, может быть незаконно изменена, похищена или уничтоженаЗакон об информационной безопасностиОсновное положение Во Франции использование информационных технологий для нарушения функционирования объектов информационной и телекоммуникационной инфраструктуры зарубежных государств является составной частью общей системы обеспечения информационной безопасности государстваНа региональном уровне существуют более развитые системы защиты данных, чем на национальном В настоящее время около 1 000 органов местного самоуправления имеют свое собственное законодательство о защите персональных данных, обрабатываемых местными административными органами Большинство этих местных законов содержит положения, подобные положениям национального закона Однако имеется около 100 местных правительств, которые приняли более современное и развитое, чем на национальном уровне, законодательство о защите данных, основанное на Руководящих принципах ОЭСРТаким образом, проблема обеспечения информационной безопасности не является сегодня узко государственной категорией, а переходит в область международных проблем, для решения которых требуется объединение ведущих мировых державБольшое внимание проблемам обеспечения международной информационной безопасности в глобальных ИТК было уделено на саммите “Большой восьмерки”, проходившем в июле 2000 года в городе Окинава (Япония) Главы государств и правительств, подписавших Окинавскую хартию глобального информационного общества, признали, что ИТК являются одним из наиболее важных факторов, влияющих на формирование общества XXI векаОдна из главных проблем обеспечения международной информационной безопасности заключается в том, что оно не является объектом регулирования международного права Осознание этого факта побудили Россию взять на себя инициативу в рамках мирового сообщества об официальной постановке вопроса правового обеспечения международной информационной безопасности

51 Принципы, силы, средства и условия организационной защиты информации

предполагающий принятие соответствующих мер на всех этапах жизненного цикла системы защиты информацииОсобое внимание необходимо уделять принципу комплексности Для обеспечения безопасности во всем многообразии структурных элементов фирмы, при множестве угроз и способов несанкционированного доступа должны применяться все виды и формы защиты и противодействия в полном объеме Недопустимо применять отдельные формы или технические средстваКомплексная безопасность предпринимательской деятельности — это обеспечение безопасности объектов защиты совокупностью выделенных для этих целей сил и средств посредством проводимых ими правовых, организационных, инженерно-технических и других мер, мероприятий и действий Комплексная безопасность предпринимательства, по совокупности элементов ее составляющих, отвечает на три главных вопроса: что защищается, кто защищает, как защищаетсяНапример, персонал организации защищается силами и средствами подразделения охраны и режима предприятия (физическая защита) проведением мероприятий инженерно-технической защиты (установка, монтаж и эксплуатация систем охранного телевидения, пожарной и охранной сигнализации и тп)Комплексность безопасности достигается объединением сил и средств физического, технического, специального и информационно-коммерческого направлений защиты при строгом соблюдении баланса интересов объектов защиты Организационная защита информации является организационным началом, так называемым «ядром» в общей системе защиты конфиденциальной информации предприятия От полноты и качества решения руководством предприятия и должностными лицами организационных задач зависит эффективность функционирования системы защиты информации в целом Среди основных направлений защиты информации наряду с организационной выделяют правовую и инженерно-техническую защиту информацииОднако организационной защите информации среди этих направлений отводится особое место Организационная защита информации призвана посредством выбора конкретных сил и средств (включающие в себя правовые, инженерно-технические и инженерно-геологические) реализовать на практике спланированные руководством предприятия меры по защите информации Эти меры принимаются в зависимости от конкретной обстановки на предприятии, связанной с наличием возможных угроз, воздействующих на защищаемую информацию и ведущих к её утечке

52 Организационные источники и каналы утечки информации

Каналы распространения информации носят объективный характер, отличаются активностью и включают в себя: • естественные технические каналы излучения, создания фона Канал распространения информации представляет собой путь перемещения сведений из одного источника в другой в санкциони­рованном (разрешенном, законном) режиме или в силу объектив­ных закономерностей Например: обсуждение важного вопроса на закрытом совещании, запись на бумаге содержания изобретения, переговоры с потенциальным партнером, работа на ЭВМ и тд Угрозы сохранности, целостности и конфиденциальности инфор­мационных ресурсов ограниченного доступа практически реализуются через риск образования канала несанкционированного получения (до­бывания) кем-то ценной информации и документов Этот канал представляет собой совокупность незащищенных или слабо защищенных фирмой направлений возможной утраты конфиденциальной информации, которые злоумышленник использует для получения необходи­мых сведений, преднамеренного незаконного доступа к защищаемой информации Каждая конкретная фирма обладает своим набором каналов несанкционированного доступа к информации, что зависит от множества моментов — профиля деятельности, объемов защищаемой информации, профессионального уровня персонала, местополо­жения здания и тп Функционирование канала несанкционированного доступа к ин­формации обязательно влечет за собой утрату информации, исчез­новение носителя информации В том случае, когда речь идет об утрате информации по вине персонала, используется термин «разглашение (огласка) информа­ции» Человек может разглашать информацию устно, письменно, с помощью жестов, мимики, условных сигналов, лично, через посредников, по каналам связи и тд Термин «утечка информа­ции», хотя и используется наиболее широко, однако в большей степени относится, по нашему мнению, к утрате информации за счет ее перехвата с помощью технических средств разведки, по техническим каналам Утрата информации характеризуется двумя условиями, информация переходит: а) непосредственно к заинтересованному лицу — конкуренту, злоумышленнику

53 Организационные основы защиты информации на предприятии

Организационная защита информации является организационным началом, так называемым «ядром» в общей системе защиты конфиденциальной информации предприятия От полноты и качества решения руководством предприятия и должностными лицами организационных задач зависит эффективность функционирования системы защиты информации в целом Среди основных направлений защиты информации наряду с организационной выделяют правовую и инженерно-техническую защиту информацииОднако организационной защите информации среди этих направлений отводится особое место Организационная защита информации призвана посредством выбора конкретных сил и средств (включающие в себя правовые, инженерно-технические и инженерно-геологические) реализовать на практике спланированные руководством предприятия меры по защите информации Эти меры принимаются в зависимости от конкретной обстановки на предприятии, связанной с наличием возможных угроз, воздействующих на защищаемую информацию и ведущих к её утечке Роль руководства предприятия в решении задач по защите информации трудно переоценитьд Цель принимаемых руководством предприятия и должностными лицами организационных мер - исключение утечки информации и, таким образом, уменьшение или полное исключение возможности нанесения предприятию ущерба, к которому эта утечка может привести Используются два примерно равнозначных определения организационной зашиты информацииОрганизационная защита информации - составная часть системы защиты информации, определяющая и вырабатывающая порядок и правила функционирования объектов защиты и деятельности должностных лиц в целях обеспечения защиты информации Организационная защита информации на предприятии - регламентация производственной деятельности и взаимоотношений субъектов (сотрудников предприятия) на нормативно-правовой основе, исключающая или ослабляющая нанесение ущерба данному предприятию Первое из приведённых определений в большей степени показывает сущность организационной защиты информации Второе - раскрывает её структуру на уровне предприятия Вместе с тем оба определения подчёркивают важность нормативно-правового регулирования вопросов защиты информации наряду с комплексным подходом к использованию в этих целях имеющихся сил и средств

54 Допуск и доступ к конфиденциальной информации и документам

Этой системой должно быть четко и однозначно определено: кто, кого и к каким сведениям, когда и как допускаетРазграничение доступа основывается на однозначном расчленении информации по тематическим группам и пользователям, которым эта информация необходима для работы Это дает возможность разделить знание элементов конфиденциальной информации среди как можно большего числа сотрудников с целью, чтобы целиком идею не знал никтоРазрешительная система допуска к конфиденциальным документам решает следующие задачи:- допуск сотрудника к конфиденциальной информации;- непосредственный доступ сотрудника к конкретным сведениямПод допуском понимается процедура оформления права сотрудника фирмы или иного лица на доступ к сведениям ограниченного распространения Оформление допуска – согласие лица на определенные ограничения в использовании информации - всегда носит добровольный характер А само наличие допуска предоставляет сотруднику формальное право работать со строго определенным кругом конфиденциальных документов, баз данных и отдельных сведенийНа сотрудников, оформленных на допуск по третьей форме, кадровым отделом составляются общие списки лиц или списки по каждому лицу отдельно Карточки этих сотрудников хранятся в подразделении по защите конфиденциальных сведений вместе с договором об оформлении допуска в специальной картотеке В карточке также указывается номер списка и дата утверждения руководителем этого списка, они заверяются подписью руководителя, его печатью и регистрируются в журнале учета карточек Кстати, сама карточка с момента заполнения является конфиденциальным документом и уничтожается так же, как и списки, по истечении одного года после увольнения сотрудникаКонечной инстанцией, решающей вопрос о необходимости предоставления допуска данному лицу, является руководитель, который распоряжается этой информацией и осуществляет за ней контроль Решение о допуске оформляется распоряжением руководителя организации с соответствующей отметкой в карточке (либо в списке лиц) и заверяется его подписью и печатью организации

55 Направления и методы работы с персоналом предприятия, допущенным к конфиденциальной информации

Проведен анализ методик работы с персоналом, имеющем доступ к конфиденциальной информации, акцентируется внимание на комплексном подходе Проанализированы характерные особенности основных этапов, на которых осуществляется взаимодействие с персоналом, исходя из особенностей структуры организации и отраслевой специфики Выявлена и обоснована необходимость постоянной, планомерной и динамичной работы соответствующих подразделений с сотрудниками органов государственной власти, государственных учреждений и предприятийПроведен анализ методик работы с персоналом, имеющем доступ к конфиденциальной информации, акцентируется внимание на комплексном подходе Проанализированы характерные особенности основных этапов, на которых осуществляется взаимодействие с персоналом, исходя из особенностей структуры организации и отраслевой специфики Выявлена и обоснована необходимость постоянной, планомерной и динамичной работы соответствующих подразделений с сотрудниками органов государственной власти, государственных учреждений и предприятийКлючевые слова: персонал, защита конфиденциальной информации, управление персоналом, методы управления персоналомОдним из наиболее актуальных и важных направлений в деятельности руководства является постоянная работа с персоналом предприятия, имеющим в силу своих должностных обязанностей доступ к конфиденциальной информации Персонал, постоянно работающий со сведениями конфиденциального характера (их носителями), — основной субъект правоотношений в сфере защиты конфиденциальной информации Одновременно он и единственный ее «нематериальный носитель» В решении проблемы комплексной защиты информации на предприятии все более значительное место занимает выбор эффективных способов и методов работы с персоналомВ обобщенном виде можно представить несколько основных этапов работы с сотрудниками предприятия, независимо от степени конфиденциальности информации, к которой данные сотрудники допущены (допускались или будут допускаться):Анализ коэффициента текучести позволит формировать структуру кадров исходя из:

56 Организация охраны предприятий

Инструкция по   
 организации охраны предприятия (фирмы или организации) (статус   
 предприятия) по   
 организации охраны предприятия (объединения) Настоящая   
 Инструкция устанавливает единые требования по обеспечению   
 безопасности предприятия путем комплексной охраны его   
 объектов, территорий и материальных ценностей  
 Охрана предприятия осуществляется на основе контракта   
 (договора) с юридическим лицом, имеющим право заниматься   
 частной охранной деятельностью I Цель   
 охраны поставить   
 под надежную защиту ведущие отношения предприятия как внутри   
 него, так и в сфере его предпринимательской деятельности;   
 Формулировка "цели" требует выделения "ведущих отношений"   
 внутри предприятия и в сфере его " предпринимательства То   
 есть речь идет о таких видовых связях, без которых немыслимо   
 само существование предприятия, его нормальная жизнь и   
 деятельность, а также его модернизация "Ведущие отношения"   
 необходимо искать в характере предпринимательства предприятия,   
 в особенностях его, объектов, территорий, персонала и   
 материальных ценностей, подлежащих охране  
 а) стационарные объекты предприятия: здания; сооружения;   
 коммуникации; средства производства; б)   
 подвижные объекты частного предприятия: транспортные средства;   
 информация; персонал; грузы; маршруты передвижения; деловые   
 встречи; бизнес мероприятия; денежные средства, ценные бумаги   
 и драгоценности и др II   
 Задачи охраны 1   
 Контроль объекта, закрытой территорий' и территории   
 ограниченного доступа (в  масштабах предприятия) с

57 Организация внутриобъектового и пропускного режимов на предприятии

Основная задача руководства предприятий, офисных зданий и прочих объектов – организация различных мер для безопасности жизни сотрудников, защита имущества объекта и внутренней информации Для этого на объектах детально прорабатывается и внедряется целый комплекс различных мероприятий Одна из основных мер – правильная организация внутриобъектового и пропускного режима  Что это такое и для чего это нужно?Для правильной организации внутриобъектового режима важна строгая отчетность Если на объекте нет специальных цифровых носителей, то сотрудники охраны заполняют специальные журналы и бланки, в которых помимо учета рабочего времени сотрудников и регистрации посетителей отражается также ввоз и вывоз имущества, графики дежурств и прием/сдача помещений под охрануПомимо внутриобъектового режима важную роль играет и пропускной режим Он также предполагает комплекс различных мер, направленных на:Организация пропускного режима на предприятии или ином объекте – это один из ключевых моментов при обеспечении мер по безопасности объекта и прилегающей территории Для этого устанавливают контрольно-пропускные пункты (КПП) – специальные помещения на территории объекта, оснащенные системами контроля доступа, физическими барьерами, видеонаблюдением, пунктом охраныТребования и правила по обоим режимам организация должна донести до каждого сотрудника объекта Как это происходит?Приказ и положение создаются и вводятся директором объекта В Приказе указываются ответственные лица (менеджер по персоналу, начальник службы безопасности), проставляются даты начала ввода режима и сроки ознакомления сотрудников с новыми правилами Положение об организации режимов включает в себя всю информацию о введении обоих режимов Нарушение правил грозит административными расследования и штрафами о внутриобъектовом, пропускном режиме и охране ОГБУЗ ИОИКБ 33 Обязанности пользователей пропускного режима 56 Охрана общественного порядка, контроль въезда (выезда) автотранспорта, обеспечение пропускного режима и выполнение санитарно-эпидемиологических правил

58 Требования к помещениям, в которых проводятся работы с конфиденциальной информацией или хранятся носители информации

К помещениям, предназначенным для ведения работ с использованием сведений, составляющих государственную тайну, или для хранения их носителей, предъявляется ряд требований На практике данные требования, как правило, распространяются на служебные помещения и хранилища предприятия, в которых используются в работе или хранятся не только названные сведения, но и другие виды конфиденциальной информации (или ее носители) Это позволяет обеспечить сохранение конфиденциальности проводимых в указанных помещениях работ, а также надежную сохранность носителей конфиденциальной информацииРазмещение и оборудование указанных режимных помещений должны исключать возможность бесконтрольного проникновения в них посторонних лиц и гарантировать сохранность находящихся в них носителей конфиденциальной информации Поэтому к данным помещениям предъявляются особые требования режима секретностиРежимные помещения, в которых в нерабочее время хранятся носители конфиденциальной информации, оснащаются охранной сигнализацией, связанной с караульным помещением, пультом централизованного наблюдения за сигнализацией службы охраны или с дежурным по предприятиюРежимные помещения, в которых имеются технические средства, разрабатываются, испытываются или эксплуатируются специальные изделия, имеющие охраняемые характеристики, оборудуются в соответствии с требованиями по противодействию иностранным техническим разведкам и технической защите информацииПеред началом эксплуатации режимные помещения обследуются комиссией, назначаемой руководителем предприятия, и аттестуются на соответствие требованиям, предъявляемым к помещениям для проведения работ с конкретным видом конфиденциальной информации Результаты работы комиссии оформляются актом пригодности помещения для проведения конкретных видов работ, утверждаемым руководителем предприятия Обследование и аттестация режимных помещений проводится не реже одного раза в 5 лет, а также после их ремонта или реконструкцииДля хранения носителей конфиденциальной информации помещения обеспечиваются необходимым количеством хранилищ, замки которых оборудуются приспособлениями для опечатывания Хранилища и ключи от хранилищ учитываются в службе безопасности (режимно-секретном подразделении) Хранилища, а также входные двери помещений, в которых они находятся, оборудуются надежными замками с двумя экземплярами ключей от них, один из которых в опечатанном пенале (пакете) хранится у руководителя службы безопасности (режимно-секретного подразделения) Второй экземпляр ключей в опечатанном виде хранится у руководителя предприятия или у его заместителя

59 Организация подготовки и проведения совещаний и заседаний по конфиденциальным вопросам

Меры по защите конфиденциальной информации в ходе подготовки и проведения совещания, принимаемые руководством предприятия, должны быть как организационными, так и организационно-техническими Мероприятия по защите информации проводятся при подготовке, в ходе проведения и по окончании совещания 1 Определение состава участников и их оповещение — порядок формирования списка лиц, привлекаемых к участию в совещании, и перечня предприятий, которым необходимо направить запросы с приглашениями; порядок подготовки и направления таких запросов, формирования их содержания 4 Организация пропускного режима на территории и в служебных, помещениях, в которых проводится совещание — виды пропусков и проставляемых на них условных знаков или шифров для прохода в конкретные служебные помещения; порядок их учета, хранения, выдачи и выведения из действия, сроки уничтожения; 5 Организация допуска участников совещания к рассматриваемым вопросам — мероприятия, касающиеся непосредственного допуска участников к вопросам, выносимым на совещание, с учетом порядка их обсуждения и степени конфиденциальности информации, к которой допущен каждый участник совещания 8 Организация учета, хранения, выдачи и рассылки материалов совещания — порядок учета, хранения, размножения, выдачи, рассылки и уничтожения материалов совещания Особое внимание уделяется электронным носителям 10 Проверка и обследование места проведения совещания после его окончания — мероприятия по организации и проведению визуальной проверки, а также проверки с использованием специальных технических средств помещений 11 В плане также указываются время и место проведения совещания, состав участников, перечень предприятий, участвующих в совещании Для каждого мероприятия, включаемого в план, определяют срок (время) его проведения и ответственное за его выполнение должностное лицо (подразделение)Обе цели успешно достигаются при условии тщательной подготовки к предстоящим переговорам и установившихся в фирме порядке и правилах их ведения В практике коммерческой деятельности обычно переговоры ведутся лично и по средствам связи (телефону)

60 Порядок доступа к конфиденциальной информации командированных лиц

Доступ командированных лиц к коммерческой тайне на пред­приятиях, куда они командируются, осуществляется в порядке, определяемом обладателем информации, составляющей коммер­ческую тайну, в соответствии с установленным режимом ком­мерческой тайны Порядок доступа лиц к конфиденциальной ин­формации иного характера в каждом конкретном случае устанавливается ее обладателем, наделенным соответствующими полно­мочиямиОснованиями для доступа командированного лица к сведени­ям, составляющим государственную тайну, и их носителям явля­ются следующие документы:Порядок оформления справки о допуске и предписания на выполнение задания определен в Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государ­ственной тайнеПостоянная работа с персоналом предприятия, имеющим до­ступ к конфиденциальной информации, — одно из наиболее ак­туальных и важных направлений в деятельности руководства и должностных лиц предприятия Персонал, постоянно работающий со сведениями конфиденциального характера (их носителями), — основной субъект правоотношений в сфере защиты конфиденци­альной информации Одновременно он и единственный ее «нема­териальный носитель» В решении проблемы комплексной защиты информации на предприятии все более значительное место зани­мает выбор эффективных способов и методов работы с персона­лом Являясь генератором новых идей, открытий и изобретений, ускоряющих научно-технический прогресс, персонал направляет максимальные усилия на повышение благосостояния предприя­тия в целом и каждого его сотрудника в частностиПричинами разглашения конфиденциальной информации допу­щенным к ней персоналом предприятия чаще всего становятся следующие факторы и обстоятельства:- слабый контроль со стороны руководителей всех уровней за состоянием защиты информации и эффективностью принимае­ мых мер по недопущению утечки этой информации;- недостаточное внимание к вопросам организации работы с персоналом предприятия, изучению морально-деловых качеств сотрудников предприятия, допущенных к конфиденциальной информации;

61 Защита информации при осуществлении международного сотрудничества и вы- езде персонала предприятия за границу

В настоящем учебном пособии изложены вопросы организационно-правовой оценки защиты информации в органах государственной власти, на предприятиях и в организациях различных форм собственности, коммерческих организациях и учреждениях Рассмотрены понятия конфиденциальности информации, принципы и критерии отнесения информации к коммерческой тайне, вопросы организации допуска и доступа персонала к конфиденциальной информации, основные (Подробнее)направления и методы работы по организации допуска к конфиденциальной информации, по организации совещаний, в ходе издательской и рекламной деятельности, также рассмотрены вопросы аналитической работы и контроля состояния защиты конфиденциальной информации Данное учебное пособие рекомендуется для изучения руководителям и специалистам по информационным технологиям и защите информации коммерческих структурБизнес книгиЭкономика > Экономика предприятия ; Менеджмент Маркетинг Коммерция Реклама КонтроллингЭкономика > Экономика предприятия ; Менеджмент Маркетинг Коммерция Реклама КонтроллингПраво Юридические наукиТехника > Кибернетика > Теория информации ; Вычислительная техника КомпьютерыКомпьютеры Информатика Интернет > Информационная безопасность ; Програмное обеспечениеДля специалистов, научных работниковУчебные издания > ОсновыТехника > Кибернетика > Теория информации ; Вычислительная техника КомпьютерыКомпьютеры Информатика Интернет > Информационная безопасность ; Програмное обеспечениеДля специалистов, научных работниковУчебные издания > ОсновыКомпьютеры Информатика Интернет > Информационная безопасность ; Програмное обеспечениеДля специалистов, научных работниковУчебные издания > ОсновыДля специалистов, научных работниковУчебные издания > ОсновыУчебные издания > ОсновыКонец информации — это конец света  
 В  
 Организаторские функции руководителей предприятия играют важную роль в достижении основных целей его деятельностиВ  
 Организаторские функции руководителей предприятия играют важную роль в достижении основных целей его деятельности Не случайно выбор управленческих решений не может быть эффективным без строгой системы применения нормативно-методических документов на основе опыта работы предприятия в той или иной области, в нашем случае — области, связанной с защитой конфиденциальной информации

62 Защита информации при публикаторской и рекламной деятельности

Защита информации при проведении мероприятий электронного характераЗащита информации при публикаторской деятельностиОрганизация подготовки материалов к открытому опубликованиюРаботу современной фирмы невозможно представить без публикаторской деятельности и рекламных акций различного характера Вместе с тем, если фирма работает с конфиденциальной информацией, то могут появиться причины к возникновению каналов утечки этой информации Мероприятия по защите информации в процессе подготовки и реализации рекламных и публикаторских (издательских) проектов должны занимать особое место в деятельности фирмы С учетом положений законодательства РФ о рекламе фирма может осуществлять следующие основные виды рекламной деятельности:Основными направлениями защиты информации в ходе рекламной деятельности являются:подготовка и экспертиза материалов, предназначенных для использования в рекламной деятельности, на предмет отсутствия у них информации с ограниченным доступом;При получении запроса из антимонопольного органа руководитель фирмы организует предоставление в установленный срок запрашиваемой информации и направление органу, приславшему запрос, письменного уведомления о невозможности ее распространения без согласия фирмы, являющейся обладателем информацииУсилия службы безопасности фирмы при осуществлении публикаторской деятельности направляются на исключение утечки конфиденциальной информации С этой целью на предприятии разрабатывается инструкция, определяющая задачи в данной области для всех должностных лиц и структурных подразделений фирмыОсновными направлениями защиты информации в ходе публикаторской деятельности являются:определение тематики издаваемых материалов в целях исключения из них тематики, содержащих конфиденциальную информацию, подготовки рекомендаций по исключению из них иной актуальной информации, распространение которой может нанести ущерб предприятию;В целях недопущения утечки информации о деятельности фирмы, содержащей сведения конфиденциального характера, на фирме планируется и проводится работа по анализу содержания материалов, предназначенных для открытого распространения В рамках этой работы служба безопасности, режимно-секретное подразделение или специально создаваемое в структуре фирмы подразделение (специально назначенное должностное лицо) планирует и осуществляет комплекс организационных мероприятий Сотрудники фирмы, принимающие непосредственное участие в подготовке материалов к открытому опубликованию, должны руководствоваться положениями ст 5 Закона РФ «О государственной тайне», Перечнем сведений, отнесенных к государственной тайне, другими нормативными правовыми актами, а также перечнем сведений, составляющих коммерческую тайну фирмы

63 Организация служебного расследования по фактам разглашения конфиденциальной информации или утраты носителей информации

Организация служебного расследования по фактам разглашения конфиденциальной информации или утраты носителей информации Ответственность за разглашение конфиденциальной информации и утрату носителей информации Разглашение конфиденциальной информации — предание огласке этой информации работником, допущенным к ней в связи с выполнением функциональных (должностных) обязанностей За разглашение конфиденциальной информации, утрату носителей конфиденциальной информации и нанесение вследствие этих действий ущерба предприятию (работодателю) виновные лица привлекаются к дисциплинарной, материальной, административной или уголовной ответственностиОпределенные ст 192 Трудового кодекса РФ: замечание, выговор, увольнение по соответствующим основаниям Порядок применения дисциплинарных взысканий определен в ст 193 кодекса Увольнение работника осуществляется в соответствии с положениями ст 1 ОРГАНИЗАЦИЯ СЛУЖЕБНОГО РАССЛЕДОВАНИЯ ПО ФАКТАМ РАЗГЛАШЕНИЯ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ ИЛИ УТРАТЫ НОСИТЕЛЕЙ ИНФОРМАЦИИ Служебное расследование должно проводиться в предельно короткий срок (не более месяца со дня обнаружения факта разглашения конфиденциальной информации или утраты ее носителей)Введение 31 Что такое конфиденциальная и служебная информация? 42 Проведение служебного расследования по фактам утечки конфиденциальной информации, утраты носителей, содержащих такие сведения, а так же по фактам иных нарушений режима конфиденциальности 52  «Организация и методология служебного расследования по фактам нарушения правил защиты конфиденциальной и служебной информации»             В состав комиссии входят не  менее трех человек (включая  работника режимно-секретного подразделения), имеющих непосредственное отношение  к данным сведениям и допуск к государственной тайне по соответствующей форме (соответствующий допуск к конфиденциальной информации) При необходимости указанные работники освобождаются от исполнения своих служебных обязанностей на время проведения служебного расследования В работе комиссии могут принимать участие представители вышестоящей организации (если она имеется)

64 Организация аналитической работы по предупреждению утечки конфиденциальной информации

Аналитические методы обработки информации очень важны и успешно используются большинством фирм Не в последнюю очередь в аналитической обработке нуждаются сведения, получаемые и используемые службой безопасности фирмы Такие сведения отрывочны, противоречивы, зачастую недостоверны, но именно на их основе принимаются жизненно важные для фирмы решенияРуководитель каждой фирмы имеет собственный взгляд на построение, направления работы и структуру информационно-аналитической службы (ИАС) На основе многолетнего опыта работы в этой области как отечественных, так и зарубежных специалистов сформировалось мнение, что в силу определенных причин наиболее эффективно такие службы функционируют как ядро службы безопасности В первую очередь это объясняется тем, что основным потребителем аналитически обработанных данных является сама служба безопасности как подразделение, наиболее нуждающееся в аналитически обработанных данных, работающее на опережение и прогнозирование событий Кроме того, в ходе аналитической работы очень часто используются (или могут быть получены) конфиденциальные сведения, что также подтверждает рациональность размещения ИАС в службе безопасности Даже не являющиеся конфиденциальными аналитически обработанные данные представляют собой наиболее ценные информационные ресурсы фирмыЗащита информации внутри ИАС представляет собой крайне сложную задачу, так как специфика аналитической работы в ряде случаев вступает в прямое противоречие с нормами защиты информации Например, обеспечение такого важного принципа, как дробление информации в работе реальных ИАС, в большинстве случаев практически невозможно, так как это тормозит работу всей системы ИАС, где сотрудники должны иметь представление обо всей картине событий Сокрытие какой-либо информации от сотрудников ИАС может привести их к ложным выводам, а фирму — к принятию неверных решений, следовательно, и к убыткам ИАС, являясь ядром службы безопасности фирмы, не имеет и не должна иметь властных функций Такое положение исключает намеренное искажение обрабатываемой информации и позволяет работать «на стыках» по пограничным вопросам

65 Планирование процессов организационной защиты информации

Одно из наиболее важных направлений деятельности предприятия, осуществляющего работу со сведениями конфиденциального характера, - планирование мероприятий по защите конфиденциальной информации Планирование указанных мероприятий занимает особое место в системе управления деятельностью как предприятия в целом, так и его структурных подразделений (отдельных должностных лиц) Трудно также переоценить значение этого направления в общей системе организационных мер обеспечения информационной безопасности предприятияОсновными целями планирования мероприятий по защите информации являются:· организация проведения комплекса мероприятий по защите конфиденциальной информации, направленных на исключение возможных каналов утечки этой информации;· установление персональной ответственности всех должностных лиц предприятия за решение вопросов защиты информации в ходе производственной и иной деятельности предприятия;определение сроков (времени, периода) проведения конкретных мероприятий по защите информации;· систематизация (объединение) всех проводимых на плановой основе мероприятий по различным направлениям защиты конфиденциальной информации;· установление системы контроля за обеспечением защиты информации на предприятии, а также системы отчетности о выполнении конкретных мероприятий;Основой для планирования мероприятий по защите информации на предприятии служат:Планирование мероприятий по защите конфиденциальной информации проводится одновременно с планированием основной производственной и иной деятельности предприятия Планирование может осуществляться на календарный год, календарный месяц, неделю, а также на иной определенный срок, обусловленный проведением важных мероприятий (работ) по видам деятельности предприятия, если они связаны с вопросами конфиденциального характера Планы мероприятий, разрабатываемые на срок более одного календарного года, относятся, как правило, к стратегическому планированию, остальные планы решают тактические задачи Такими программами могут быть реконструкция предприятия, внедрение новых технологий, в том числе информационных, и тп

66 Организация контроля состояния защиты конфиденциальной информации на предприятии

Контроль состояния защиты подразделяется на: Контроль заключается в проверке выполнения актов законодательства Российской Федерации по вопросам защиты информации, а также в оценке обоснованности и эффективности принятых мер защиты для обеспечения выполнения утвержденных требований и норм по защите информации Основная задача контроля – предупреждение нарушений установленных требований и правил в области защиты информации и выработка рекомендаций по совершенствованию объектовой системы защиты информации Контроль состояния защиты информации складывается из контроля организации защиты информации и контроля эффективности защиты информации Согласно ГОСТ Р50922-96 «Защита информации Термины и определения»: Контроль состояния защиты информации – проверка соответствия организации и эффективности защиты информации установленным требованиям и/или нормам в области защиты информации Контроль организации защиты информации – проверка соответствия состояния организации, наличия и содержания документов требованиям правовых, организационно-распорядительных и нормативных документов по защите информации Контроль эффективности защиты информации – проверка соответствия эффективности мероприятий по защите информации установленным требованиям или нормам эффективности защиты информации Организационный контроль эффективности защиты информации заключается в выявлении предпосылок к утечке защищаемой информации, технический контроль эффективности защиты информации – в выявлении технических каналов утечки защищаемой информации Инструментальный метод заключается в проведении определенных измерений с помощью аппаратуры контроля с целью проверки эффективности защиты информации Экспертный метод заключается в проведении проверок средства вычислительной техники на наличие подключений к сетям международного информационного обмена и обработки информации ограниченного доступа Результаты технического контроля оформляются в виде протокола, подписываются представителем органа контроля и представителем организации Проверке подлежит объектовая система защиты информации

67 Государственные, национальные и отраслевые стандарты по информационной безопасности

ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология Методы и средства обеспечения безопасности Часть 1 Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий Information technologyСТО БР ИББС-10-2010 Стандарт Банка России Обеспечение информационной безопасности организаций банковской системы Российской Федерации Общие положения СТО БР ИББС-1Подборка ГОСТов, российских национальных (государственных) и отраслевых стандартов в области информационной безопасности (© ЗАО НПО Эшелон, 2010 г)ГОСТ Р 52611–2006 Системы промышленной автоматизации и их интеграция Средства информационной поддержки жизненного цикла продукции Безопасность информации Основные положения и общие требованияСогласно сообщению Министерства связи и информационных технологий Азербайджана рассмотрено принятие 4 национальных стандартов по информационной безопасности, разработанных на основании международных стандартов ISO/IEC 27001:2005, ISO/IEC 27005:2008, ISO/IEC 11770-1:1996 и ISO/IEC TR 18044:2004[…]  В прошлогодней подборкой национальных и ведемственных стандартов РФ можно ознакомиться на нашем блоге: Российские стандарты по информационной безопасности […]Стандарты информационной безопасности – это обязательные или рекомендуемые к выполнению документы, в которых определены подходы к оценке уровня ИБ и установлены требования к безопасным информационным системам Стандарты в области информационной безопасности выполняют следующие важнейшие функции: - выработка понятийного аппарата и терминологии в области информационной безопасности - формирование шкалы измерений уровня информационной безопасности - повышение технической и информационной совместимости продуктов, обеспечивающих ИБ - накопление сведений о лучших практиках обеспечения информационной безопасности и их предоставление различным группам заинтересованной аудитории – производителям средств ИБ, экспертам, ИТ-директорам, администраторам и пользователям информационных систем Благодаря стандартам информационной безопасности:

68 Международные стандарты информационной безопасности

Рассмотрим наиболее известные международные стандарты в области защиты информации, которые могут быть использованы в отечественных условияхМеждународный стандарт ISO/IEC 17799:2000 (BS 7799-1:2000) «Управление информационной безопасностью — Информационные технологии» («Information technology — Information security management\*) является одним из наиболее известных стандартов в области защиты информации В соответствии с положениями этого стандарта также регламентируется процедура аудита КИСДополнительные рекомендации для управления информационной безопасностью содержат руководства Британского института стандартов — British Standards Institution (BSI), изданные в 1995—2003 гг   
 Эта статья была опубликована Воскресенье, 9 августа, 2009 at 16:56 в рубрике Стандарты информационной безопасности  
 Вы можете следить за ответами через RSS 20 feed  
 Стандарты информационной безопасности – это обязательные или рекомендуемые к выполнению документы, в которых определены подходы к оценке уровня ИБ и установлены требования к безопасным информационным системам Стандарты в области информационной безопасности выполняют следующие важнейшие функции: - выработка понятийного аппарата и терминологии в области информационной безопасности - формирование шкалы измерений уровня информационной безопасности - повышение технической и информационной совместимости продуктов, обеспечивающих ИБ - накопление сведений о лучших практиках обеспечения информационной безопасности и их предоставление различным группам заинтересованной аудитории – производителям средств ИБ, экспертам, ИТ-директорам, администраторам и пользователям информационных систем Благодаря стандартам информационной безопасности: Основными областями стандартизации информационной безопасности являются: Стандарты информационной безопасности имеют несколько классификаций: Различные классификации стандартов информационной безопасности Существуют российские стандарты информационной безопасности (ГОСТ Р ИСО/МЭК 15408, ГОСТ Р 51275 и др

69 Термины, определения и основы методологии в области технической защиты информации

Защита информацииЦели и принципы стандартизации в Российской Федерации установлены Федеральным законом от 27 декабря 2002 г N 184-ФЗ "О техническом регулировании", а правила применения национальных стандартов Российской Федерации - ГОСТ Р 10-2004 "Стандартизация в Российской Федерации Основные положения"1 РАЗРАБОТАН Федеральным государственным учреждением "Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю" (ФГУ "ГНИИИ ПТЗИ ФСТЭК России")4 В настоящем стандарте реализованы нормы Федеральных законов от 27 июля 2006 г N 149-ФЗ "Об информации, информационных технологиях и о защите информации" и от 29 июля 2004 г N 98-ФЗ "О коммерческой тайне"Настоящий стандарт устанавливает основные термины с соответствующими определениями, применяемые при проведении работ по стандартизации в области защиты информации211 защита информации; ЗИ: Деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию221 правовая защита информации: Защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением222 техническая защита информации; ТЗИ: Защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств223 криптографическая защита информации: Защита информации с помощью ее криптографического преобразования224 физическая защита информации: Защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты

70 Характеристика информации и информационных процессов как предмета технической защиты

Информация, информационные процессы и информационное общество Информация Информация относится к фундаментальным, неопределяемым понятиям науки информатика Термин «информация» происходит от латинского слова information, что означает сведения, разъяснения, изложение  
 Во многом определение информации зависит от отрасли человеческой деятельности: - в бытовом смысле под информацией понимают любые данные или сведения, которые кого-либо интересуют Например, сообщение о каких-либо событиях, о чей-либо деятельности и тп Информация относится к фундаментальным, неопределяемым понятиям науки информатика Термин «информация» происходит от латинского слова information, что означает сведения, разъяснения, изложение  
 Во многом определение информации зависит от отрасли человеческой деятельности: - в бытовом смысле под информацией понимают любые данные или сведения, которые кого-либо интересуют Например, сообщение о каких-либо событиях, о чей-либо деятельности и тпОбеспечение информационной безопасности (ИБ) — одна из ключевых мер по поддержанию стабильной работы компаний и промышленных предприятий, государственных органов и общественных организаций, функционирования экономики и государства в целом Учитывая ее все возрастающее значение, ИБ регламентируется на уровне федерального законодательства и по праву считается одним из элементов национальной безопасности Основным законодательным актом в этой сфере является федеральный закон № 187-ФЗВ законе, помимо прочего, дается определение критической информационной инфраструктуре К информационной инфраструктуре в целом относятся информационные системы и сети телекоммуникации, АСУ и линии связи, которые обеспечивают их взаимодействиеДля отнесения объекта информационной безопасности к «критической инфраструктуре» он должен использоваться государственным органом или учреждением, российской компанией или организацией в следующих отраслях:Также к критическим объектам защиты в области информационной безопасности причисляют системы, которые обеспечивают взаимодействие вышеперечисленных организаций и компаний Важно, что они тоже должны принадлежать российским компаниям или предпринимателям

71 Характеристика угроз безопасности информации в автоматизированных информационных системах

Иванов, К К Угрозы безопасности информации в автоматизированных системах / К К Иванов, Р Любая автоматизированная система управления, кроме выполнения своих прямых задач, должна также обеспечивать безопасность информации, хранящейся в ней, то есть ее защищенность при получении, обработке, хранении, передаче и использовании от различного вида угроз [1] Любой вид угрозы безопасности в автоматизированных системах направлен на нарушение достоверности, сохранности и конфиденциальности информации Все эти угрозы могут воздействовать либо на аппаратные средства, либо на программные средства, либо на самих носителей информации Рис 1 Классификация угроз безопасности автоматизированным системам Следующим видом непреднамеренных угроз безопасности системы являются ошибки при разработке системы и ошибки в комплексах алгоритмов и программ (системные, алгоритмические, программные или технологические) Ущерб данного вида угроз аналогичен ущербу при сбоях и отказах технических средств Также не к непреднамеренным угрозам относятся ошибки пользователей и обслуживающего персонала Данная группа доминирует над остальными по числу угроз Подобные ошибки могут быть вызваны, например, состоянием человека, несовершенством системы или безответственным отношением к работе Чаще всего такие ошибки влекут за собой нарушение целостности и конфиденциальности информации [1] Преднамеренные угрозы являются куда более опасными, чем непреднамеренные, так как данные могут быть не только уничтожены, но еще и захвачены злоумышленниками Первым видом преднамеренных угроз являются шпионаж и диверсии Серьезный ущерб безопасности информации в системе может нанести съем электромагнитных излучения и наводок, благодаря которым можно перехватить информацию Подобное возможно из-за того, что при обработке и передаче информации создается электромагнитное поле и наводятся электрические сигналы в линиях связи Жизненный цикл автоматизированных систем (ЖЦ АС) носит итерационный характер, в процессе его развития для минимизации накопления ошибок необходимо своевременно актуализировать информационную модель объекта в соответствии с фактической обстановкой

72 Технические каналы утечки информации, обрабатываемой средствами вычисли- тельной техники и автоматизированными системами

В статье приведена классификация технических каналов утечки информации, обрабатываемой средствами вычислительной техникиСовременный этап развития общества характеризуется возрастающей ролью информационной сферы, представляющей собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информацииИнформация в зависимости от категории доступа к ней подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа) [6] К информации ограниченного доступа относится информация, составляющая государственную тайну, а также сведения конфиденциального характера (персональные данные, сведения, составляющие коммерческую, служебную и иную тайну, и тд)В соответствии с требованиями федеральных законов информация ограниченного доступа подлежит защитеПерехватом информации называется неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, приём и обработку информативных сигналов [8]В результате перехвата информации возможно неправомерное ознакомление с информацией или неправомерная запись информации на носительИсточником информативных сигналов, то есть сигналов, по параметрам которых может быть определена защищаемая информация, являются технические средства, осуществляющие обработку информации Термин «обработка информации» является обобщённым и подразумевает совокупность операций сбора, накопления, ввода, вывода, приёма, передачи, записи, хранения, регистрации, уничтожения, преобразования и отображения информации [5]д Данные технические средства и системы в ряде случаев именуются основными техническими средствами и системами (ОТСС)Наряду с техническими средствами и системами, обрабатывающими информацию ограниченного доступа, в помещениях, где они установлены, как правило, находятся и другие технические средства и системы, которые в обработке информации ограниченного доступа непосредственно не участвуютд); средства электронной оргтехники; системы и средства электрочасофикации и иные технические средства и системы Такие технические средства и системы называются вспомогательными техническими средствами и системами (ВТСС) [7, 9]

73 Характеристика технических каналов утечки информации, возникающих за счет побочных электромагнитных излучений и наводок

В статье приведена классификация технических каналов утечки информации, обрабатываемой средствами вычислительной техникиСовременный этап развития общества характеризуется возрастающей ролью информационной сферы, представляющей собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информацииИнформация в зависимости от категории доступа к ней подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа) [6] К информации ограниченного доступа относится информация, составляющая государственную тайну, а также сведения конфиденциального характера (персональные данные, сведения, составляющие коммерческую, служебную и иную тайну, и тд)В соответствии с требованиями федеральных законов информация ограниченного доступа подлежит защитеПерехватом информации называется неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, приём и обработку информативных сигналов [8]В результате перехвата информации возможно неправомерное ознакомление с информацией или неправомерная запись информации на носительИсточником информативных сигналов, то есть сигналов, по параметрам которых может быть определена защищаемая информация, являются технические средства, осуществляющие обработку информации Термин «обработка информации» является обобщённым и подразумевает совокупность операций сбора, накопления, ввода, вывода, приёма, передачи, записи, хранения, регистрации, уничтожения, преобразования и отображения информации [5]д Данные технические средства и системы в ряде случаев именуются основными техническими средствами и системами (ОТСС)Наряду с техническими средствами и системами, обрабатывающими информацию ограниченного доступа, в помещениях, где они установлены, как правило, находятся и другие технические средства и системы, которые в обработке информации ограниченного доступа непосредственно не участвуютд); средства электронной оргтехники; системы и средства электрочасофикации и иные технические средства и системы Такие технические средства и системы называются вспомогательными техническими средствами и системами (ВТСС) [7, 9]

74 Специально создаваемые радиоэлектронные технические каналы утечки информации

Каналы утечки информации — методы и пути утечки информации из информационной системы; паразитная (нежелательная) цепочка носителей информации, один или несколько из которых являются (могут быть) правонарушителем или его специальной аппаратурой Играют основную роль в защите информации, как фактор информационной безопасности Все каналы утечки данных можно разделить на косвенные и прямые Косвенные каналы не требуют непосредственного доступа к техническим средствам информационной системы Прямые соответственно требуют доступа к аппаратному обеспечению и данным информационной системы Примеры косвенных каналов утечки: Примеры прямых каналов утечки: Каналы утечки информации можно также разделить по физическим свойствам и принципам функционирования: В зависимости от вида каналов связи технические каналы перехвата информации можно разделить[1] Технические каналы утечки информации можно разделить на естественные и специально создаваемые Виды технических каналов утечки акустической информации:[6] Акустический канал утечки информации реализуется в следующем: Акустоэлектрический канал утечки информации, особенностями которого являются: Телефонный канал утечки информации для подслушивания телефонных переговоров (в рамках промышленного шпионажа) возможен: Индуктивный способ — за счёт электромагнитной индукции, возникающей в процессе телефонных переговоров вдоль провода телефонной линии В качестве приемного устройства съёма информации используется трансформатор, первичная обмотка которого охватывает один или два провода телефонной линии В оптическом канале получение информации возможно путём: В качестве среды распространения в оптическом канале утечки информации выступают: Безвоздушное пространство, являющееся средой распространения утечки информации, возникает при наблюдении за наземными объектами с космических аппаратов К свойствам среды распространения, влияющих на длину канала утечки, относятся: Типовые варианты оптических каналов утечки информации приведены в таблице Технические средства съёма информации могут быть внедрены «противником» следующими способами:

75 Технические каналы утечки акустической (речевой) информации

В случае, когда источником информации является голосовой аппарат человека, информация называется речевой Речевой сигнал является сложным акустическим сигналом, основная энергия которого сосредоточена в диапазоне частот от 300 Гц до 4000 ГцГолосовой аппарат человека является первичным источником акустических колебаний, которые представляют собой возмущения воздушной среды в виде волн сжатия и растяжения (продольных волн) Под действием акустических колебаний в ограждающих строительных конструкциях и инженерных коммуникациях помещения, в котором находится речевой источник, возникают вибрационные колебания Таким образом, в своем первоначальном состоянии речевой сигнал в помещении присутствует в виде акустических и вибрационных колебанийВ акустических каналах утечки информации средой распространения речевых сигналов является воздух, и для их перехвата используются высокочувствительные микрофоны и специальные направленные микрофоны Микрофоны соединяются с портативными звукозаписывающими устройствами или специальными  миниатюрными передатчикамиАвтономные устройства,  конструктивно объединяющие  микрофоны  и передатчики, называют закладными устройствами (ЗУ) перехвата речевой информацииПрием информации, передаваемой ЗУ, осуществляется, как правило, на специальные приемные устройства, работающие в соответствующем диапазоне длин волн Однако существуют исключения из этого правила Так, в случае передачи информации по телефонной линии с вызовом от внешнего абонента прием можно осуществлять с обычного телефонного аппаратаВ виброакустических каналах утечки информации средой распространения речевых сигналов являются ограждающие строительные конструкции помещений (стены, потолки, полы) и инженерные коммуникации (трубы водоснабжения, отопления, вентиляции и тп) Для перехвата речевых сигналов в этом случае используются вибродатчики (акселерометры)По виброакустическому каналу также возможен перехват информации с использованием «стетоскопных» ЗУ В них, как правило, для передачи информации используется радиоканал,   поэтому   такие   устройства   часто   называют радиостетоскопами Реально, также возможно использование ЗУ с передачей информации по оптическому каналу инфракрасном диапазоне  волн, а также по ультразвуковому каналу (по инженерным коммуникациям)

76 Прямые акустические каналы утечки речевой информации

Каналы утечки информации — методы и пути утечки информации из информационной системы; паразитная (нежелательная) цепочка носителей информации, один или несколько из которых являются (могут быть) правонарушителем или его специальной аппаратурой Играют основную роль в защите информации, как фактор информационной безопасности Все каналы утечки данных можно разделить на косвенные и прямые Косвенные каналы не требуют непосредственного доступа к техническим средствам информационной системы Прямые соответственно требуют доступа к аппаратному обеспечению и данным информационной системы Примеры косвенных каналов утечки: Примеры прямых каналов утечки: Каналы утечки информации можно также разделить по физическим свойствам и принципам функционирования: В зависимости от вида каналов связи технические каналы перехвата информации можно разделить[1] Технические каналы утечки информации можно разделить на естественные и специально создаваемые Виды технических каналов утечки акустической информации:[6] Акустический канал утечки информации реализуется в следующем: Акустоэлектрический канал утечки информации, особенностями которого являются: Телефонный канал утечки информации для подслушивания телефонных переговоров (в рамках промышленного шпионажа) возможен: Индуктивный способ — за счёт электромагнитной индукции, возникающей в процессе телефонных переговоров вдоль провода телефонной линии В качестве приемного устройства съёма информации используется трансформатор, первичная обмотка которого охватывает один или два провода телефонной линии В оптическом канале получение информации возможно путём: В качестве среды распространения в оптическом канале утечки информации выступают: Безвоздушное пространство, являющееся средой распространения утечки информации, возникает при наблюдении за наземными объектами с космических аппаратов К свойствам среды распространения, влияющих на длину канала утечки, относятся: Типовые варианты оптических каналов утечки информации приведены в таблице Технические средства съёма информации могут быть внедрены «противником» следующими способами:

77 Составные акустические каналы утечки речевой информации

Delphi site: daily Delphi-news, documentation, articles, review, interview, computer humorВ акустическом канале утечки носителем информации от источника к несанкционированному получателю является акустическая волна в атмосфере, воде и твердой среде Структура канала утечки информации приведена на рис 65Рис 65 Структура акустического канала утечки информацииАкустические речевые сигналы создает речевой аппарат человека, голосовой тракт которого представляет собой трубку со средней длиной у взрослого мужчины примерно 17 см и с переменной площадью поперечного сечения Вход в голосовой тракт образуют голосовые связки, а выход - губы Поперечное сечение может изменяться при движении артикул ярных органов - губ, челюстей, языка и небной занавески (мягкого неба), являющейся продолжением твердого неба, от полного закрытия до величины более 20 см2Акустические сигналы машин и технических средств возникают в результате колебаний их поверхностей и частиц воздуха, проходящего через различные отверстия и полости машин и средствТак как основным источником акустической речевой информации является человек, то средняя мощность (громкость) источников сигналов акустических каналов утечки информации составляет 40-80 дБАкустические волны как носители информации характеризуются следующими показателями и свойствами: д Но и в однородной среде ее параметры не постоянные, а могут существенно различаться в разных точках пространстваПри определенных условиях неоднородности создают условия для образования акустических (звуковых) каналов, по которым акустическая волна может распространяться на значительно большие расстояния, как свет по оптическим световодам Такое явление возникает потому, что скорость распространения акустической волны в воде увеличивается с глубиной из-за повышения плотности воды и уменьшается при понижении ее температуры в более глубоких слоях, особенно в летнее время В слоях ниже акустического канала преобладает влияние первого фактора, способствующего увеличению скорости акустической волны, выше- второго фактора Акустическая волна, попадающая в эту область, распространяется внутри ее с соответствующим для параметров воды затуханием

78 Способы и средства перехвата информации, передаваемой по каналам связи

В настоящее время для передачи информации используются в основном KB, УКВ, радиорелейные, тропосферные и космические каналы связи, различные виды телефонной радиосвязи (например, сотовая), а также кабельные и волоконно-оптические линии связи В зависимости от вида канала связи технические каналы перехвата информации можно разделить на электромагнитные, электрические и индукционныеЭлектромагнитный канал перехвата информации Электромагнитные излучения передатчиков средств связи, модулированные информационным сигналом, могут перехватываться портативными средствами радиоразведки Данный канал наиболее широко используется для прослушивания телефонных разговоров, ведущихся по радиотелефонам, сотовым телефонам или по радиорелейным и спутниковым линиям связиЭлектрический канал перехвата информации, передаваемой по кабельным линиям связи, предполагает контактное подключение аппаратуры перехвата к кабельным линиям связи Самый простой способ - это непосредственное параллельное подключение к линии связи Но данный факт легко обнаруживается, так как приводит к изменению характеристик линии связи за счет падения напряжения Поэтому средства перехвата подключаются к линии связи или через согласующее устройство, незначительно снижающее падение напряжения, или через специальное устройство компенсации падения напряженияКонтактный способ используется в основном для снятия информации с коаксиальных и низкочастотных кабелей связи Для кабелей, внутри которых поддерживается   повышенное  давление   воздуха,   применяются  устройства, исключающие его снижение, в результате чего предотвращается срабатывание специальной сигнализацииЭлектрический канал наиболее часто используется для перехвата телефонных разговоров Устройства, подключаемые к телефонным линиям связи и совмещенные с устройствами передачи информации по радиоканалу, часто называют телефонными закладкамиНаиболее часто используемый способ контроля проводных линий связи, не требующий контактного подключения   - индукционный В индукционном канале используется эффект возникновения вокруг кабеля связи электромагнитного поля при прохождении по нему информационных электрических сигналов,  которые перехватываются специальными индукционными датчиками Индукционные датчики используются в основном для съема информации с симметричных высокочастотных кабелей

79 Способы и средства защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами

         Базовые знания в области защиты информацииТема 1 Структура, задачи и основные функции государственной системы защиты информацииПредмет, система и методология курса обучения Цели, задачи, структура, функции и роль информационной безопасности в системе национальной безопасности Российской Федерации Указ ПРФ от 12 мая 2009 г «О стратегии национальной безопасности Российской Федерации до 2020 г» Основные термины и определения в области технической защиты информацииТема 2 Законодательная и нормативная база правового регулирования вопросов защиты информацииФедеральный закон Российской Федерации от 27 июля 2006 г№149-ФЗ «Об информации, информационных технологиях и о защите информации» Указы Президента Российской Федерации и постановления Правительства Российской Федерации, а также нормативно-методические документы ФСТЭК России, регулирующие вопросы технической защиты конфиденциальной информацииТема 3 Лицензирование деятельности в области защиты информации, сертификация средств защиты информации и аттестация объектов информатизацииПорядок лицензирования деятельности в области технической защиты конфиденциальной информации Постановление Правительства Российской Федерации от 15 августа 2006 г № 504 «О лицензировании деятельности    
   
 по технической защите конфиденциальной информации» Постановление Правительства Российской Федерации от 31 августа 2006 г № 532    
   
 «О лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации»Тема 4 Специальные требования и рекомендации по технической защите конфиденциальной информацииОсновные требования и рекомендации по защите речевой информации, циркулирующей в защищаемых помещениях Требования и рекомендации по защите информации, обрабатываемой средствами вычислительной техники Основные требования и рекомендации по защите служебной тайны Основные рекомендации по защите информации, составляющей коммерческую тайну Порядок обеспечения защиты информации при эксплуатации автоматизированных систем

80 Методы, способы и средства защиты информации от утечки за счет ПЭМИН

Защита информации от утечки через ПЭМИН осуществляется с применением пассивных и активных методов и средств Пассивные методы защиты информации направлены на: Активные методы защиты информации направлены на: Рассмотрим более подробно наиболее распространенные методы пассивной и активной защиты от ПЭМИН Как известно из предыдущих лекций, при функционировании технических средств обработки, приема, хранения и передачи информации (ТСПИ) создаются побочные токи и поля, которые могут быть использованы злоумышленником для съема информации Подводя итог, можно сделать вывод, что между двумя токопроводящими элементами могут возникнуть следующие виды связи: Одним из наиболее эффективных пассивных методов защиты от ПЭМИ является экранирование Экранирование - локализация электромагнитной энергии в определенном пространстве за счет ограничения распространения ее всеми возможными способамиВокруг элемента (пусть это будет виток) с постоянным током существует магнитное поле напряженностью H0, которое необходимо экранировать Для этого окружим виток замкнутым экраном, магнитная проницаемость µ которого больше единицы Экран намагнитится, в результате чего создастся вторичное поле, которое ослабит первичное поле вне экрана То есть силовые линии поля витка, встречая экран, обладающий меньшим магнитным сопротивлением, чем воздух, стремятся пройти по стенкам экрана и в меньшем количестве доходят до пространства вне экрана Такой экран одинаково пригоден для защиты от воздействия магнитного поля и для защиты внешнего пространства от влияния магнитного поля созданного источником внутри экрана (Рисунок 16Следует отметить, что помимо функции защиты от утечки информации через ПЭМИН, экранирование может снизить вредное воздействие электромагнитного излучения на людей и уровень шумов при работе ТСПИ Средства защиты информации по каналам ПЭМИНЗа счет побочных электромагнитных излучений и наводок (ПЭМИН), можно считывать информацию с монитора вашего компьютера (разумеется с помощью специальных технических средств) на расстоянии до 200 метров, а то и больше Также можно считывать информацию с процессора, клавиатуры, винчестера, дисковода (когда они работают, естественно) Поэтому все криптосистемы становятся почти бессмысленными если не принять соответствующих мер защиты

81 Локализация побочных электромагнитных излучений и развязывание информационных сигналов

Приведены концептуальные основы инженерно-технической защиты информации, ее основные принципы, классифицированы и определены основные методы и средства обеспечения информационной безопасности по каждому из возможных каналов утечки Приведены концептуальные основы инженерно-технической защиты информации, ее основные принципы, классифицированы и определены основные методы и средства обеспечения информационной безопасности по каждому из возможных каналов утечкиКлючевые слова: системы защиты информации, технические каналы утечки информации, побочные электромагнитные излучения и наводки, закладные устройства, сотовая связь, диктофоны, направленные микрофоны, телефонный канал передачи информации, экранирование, шумы, помехиПерехватом информации называется неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, приём и обработку информативных сигналов [1,3]В результате перехвата информации возможно неправомерное ознакомление с информацией илинеправомерная запись информации на носительОсобенности технических каналов утечки информации определяются физической природой информационных сигналов и характеристиками среды их распространения Общая классификация технических каналов утечки информации включает следующие виды каналов (рис1) [1,2]:- каналы утечки, обрабатываемой техническими средствами приема, обработки, хранения и передачи информации (ТСПИ);- каналы утечки речевой информации;- утечка информации при ее передаче по каналам связи;- технические каналы утечки видовой информацииТехнические каналы утечки информацииинформации ТКУИ с ТСПИТКУ видовой информацииРис 1 Общая классификация технических каналов утечки информацииТехнические каналы утечки информации, обрабатываемой ТСПИ- съем информации с использованием закладных устройств- перехват информации путем «высокочастотного облучения» ТСПИ5 Съём информации с использованием закладных устройствЗакладные устройства, внедряемые в СВТ, по виду перехватываемой информации можно разделить на [3,4]:

82 Энергетическое скрытие побочных электромагнитных излучений и наводок от средств вычислительной техники

43 Угрозы утечки информации по каналам побочныхВозникновение угрозы ПДн по каналам ПЭМИН возможно за счет перехвата техническими средствами побочных (не связанных с прямым функциональным значением элементов ИСПДн) информативных электромагнитных полей и электрических сигналов, возникающих при обработке ПД техническими средствами ИСПДнДля регистрации ПЭМИН используется аппаратура в составе радиоприемных устройств и оконечных устройств восстановления информацииКроме этого, перехват ПЭМИН возможен с использованием электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки ПДнКаналы утечки информации, обусловленные наводками, образуются за счет соединительных линий технических средств ИСПДн и ВТСС и посторонних проводников (в том числе цепей электропитания и заземления)Для съема информации с проводных линий могут использоваться:Для волоконно-оптической системы передачи данных угрозой утечки информации является утечка оптического излучения, содержащего защищаемую информацию, с боковой поверхности оптического волокнаПоявление новых каналов связи - сотовой связи, пейджинговых сообщений, спутниковых и беспроводных сетей передачи данных - привело к развитию специализированных систем и средств контроля и перехвата информации, ориентированных на используемые в них информационные технологии, в том числе средств:перехвата информации в каналах передачи данных вычислительных сетей 2 н и 2 з 2 н и 2 з123 Принимая и декодируя эти сигналы, можно восстановить информацию, обрабатываемую ТСНаиболее опасным (с точки зрения утечки информации за счет ПЭМИН) режимом работы ТС является вывод информации на экран монитора Принимая и декодируя эти сигналы, можно восстановить информацию, обрабатываемую ТСНаиболее опасным (с точки зрения утечки информации за счет ПЭМИН) режимом работы ТС является вывод информации на экран монитораДля защиты информации от утечки по каналу ПЭМИН необходимо в точке возможного перехвата информативных сигналов уменьшить отношение сигнал-шум, чтобы сделать невозможным перехват, обработку и анализ информативных сигналов с целью извлечения информации Это может быть достигнуто двумя способами

83 Способы и средства защиты выделенных помещений от утечки речевой информации по техническим каналам

ООО «ДСЦБИ «МАСКОМ» (входит в Холдинг МАСКОМ Восток) предлагает комплексные услуги по защите от утечки речевой конфиденциальной информации кабинетов руководителей, переговорных комнат, конференц-залов и иных помещений, предназначенных для проведения конфиденциальных мероприятийВ настоящее время широкое распространение получили средства и методы несанкционированного и негласного добывания информации Естественные каналы утечки информации образуются спонтанно, в силу специфических обстоятельств, сложившихся на объекте защиты, искусственные каналы утечки информации создаются преднамеренно с применением активных методов и способов получения информациидООО «ДСЦБИ «МАСКОМ» имеет все необходимые лицензии Для блокирования каналов утечки информации в помещениях мы применяем только сертифицированные технические СЗИ, а также проводим комплекс организационных мероприятийСтоимость услуги формируется в зависимости от параметров защищаемого помещения, актуальности каналов утечки информации и выбора способа их блокирования Приведены концептуальные основы инженерно-технической защиты информации, ее основные принципы, классифицированы и определены основные методы и средства обеспечения информационной безопасности по каждому из возможных каналов утечки Приведены концептуальные основы инженерно-технической защиты информации, ее основные принципы, классифицированы и определены основные методы и средства обеспечения информационной безопасности по каждому из возможных каналов утечкиКлючевые слова: системы защиты информации, технические каналы утечки информации, побочные электромагнитные излучения и наводки, закладные устройства, сотовая связь, диктофоны, направленные микрофоны, телефонный канал передачи информации, экранирование, шумы, помехиПерехватом информации называется неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, приём и обработку информативных сигналов [1,3]В результате перехвата информации возможно неправомерное ознакомление с информацией или

84 Методы, способы и средства защиты речевой информации от утечки по техническим каналам

III Методы и способы защиты информацииот утечки по техническим каналам31 N 78132 Для исключения утечки персональных данных за счет побочных электромагнитных излучений и наводок в информационных системах 1 класса могут применяться следующие методы и способы защиты информации:использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;размещение объектов защиты в соответствии с предписанием на эксплуатацию;333435 Приведены концептуальные основы инженерно-технической защиты информации, ее основные принципы, классифицированы и определены основные методы и средства обеспечения информационной безопасности по каждому из возможных каналов утечки Приведены концептуальные основы инженерно-технической защиты информации, ее основные принципы, классифицированы и определены основные методы и средства обеспечения информационной безопасности по каждому из возможных каналов утечкиКлючевые слова: системы защиты информации, технические каналы утечки информации, побочные электромагнитные излучения и наводки, закладные устройства, сотовая связь, диктофоны, направленные микрофоны, телефонный канал передачи информации, экранирование, шумы, помехиПерехватом информации называется неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, приём и обработку информативных сигналов [1,3]В результате перехвата информации возможно неправомерное ознакомление с информацией илинеправомерная запись информации на носительОсобенности технических каналов утечки информации определяются физической природой информационных сигналов и характеристиками среды их распространения Общая классификация технических каналов утечки информации включает следующие виды каналов (рис1) [1,2]:- каналы утечки, обрабатываемой техническими средствами приема, обработки, хранения и передачи информации (ТСПИ);- каналы утечки речевой информации;- утечка информации при ее передаче по каналам связи;- технические каналы утечки видовой информацииТехнические каналы утечки информации

85 Звукоизоляция выделенных помещений

Звукоизоляция помещений направлена на локализацию источников акустических сигналов внутри них и проводится с целью исключения перехвата акустической (речевой) информации по прямому акустическому (через щели, окна, двери, вентиляционные каналы и тд) и вибрационному (через ограждающие конструкции, трубы водо-, тепло-, газоснабжения, канализации и тд) каналам Звукоизоляция оценивается величиной ослабления акустического сигнала, которое для сплошных однослойных или однородных ограждений на средних частотах приближенно рассчитывается по формуле /5/: Звукоизоляция помещений обеспечивается с помощью архитектурных и инженерных решений, а также применением специальных строительных и отделочных материалов Одним из наиболее слабых звукоизолирующих элементов, ограждающих конструкции выделенных помещений, являются окна и двери Увеличение звукоизолирующей способности дверей достигается плотной подгонкой полотна двери к коробке, устранением щелей между дверью и полом, применением уплотняющих прокладок, обивкой или облицовкой полотен дверей специальными материалами и т д Если применение обивки двери недостаточно для обеспечения звукоизоляции, то в помещении устанавливаются двойные двери, образующие тамбур Внутренние поверхности тамбура также облицовываются поглощающими покрытиями Звукоизолирующая способность окон, как и дверей, зависит от поверхностной плотности стекла и степени прижатия притворов Звукоизоляция окон с одинарным остеклением соизмерима со звукоизоляцией одинарных дверей и недостаточна для надежной защиты информации в помещении Для обеспечения необходимой степени звукоизоляции применяется двойное или тройное остекление В случаях, когда необходимо обеспечить повышенную звукоизоляцию, применяют окна специальной конструкции (например, двойное окно с заполнением оконного проема органическим стеклом толщиной 20…40 мм) Разработаны конструкции окон с повышенным звукопоглощением на основе стеклопакетов с герметизацией воздушного промежутка между стеклами и заполнением его различными газовыми смесями или создание в нем вакуума

86 Системы и средства акустической и виброакустической маскировки

Система защиты помещений"SEL SP-55-4A"Система является техническим средством активной защиты информации по виброакустическому каналу для объектов информатизации 1 категорииНаличие интерфейса RS-485 (опция) позволяет включать его в интегрированные комплексные системы защиты информации, где удаленное управление прибором и контроль его состояния осуществляется с ПК или автономного контроллераПрибор виброакустической защиты SI-3010 предназначен для виброакустического зашумления строительных конструкций помещения при защите речевой информации от утечки по вибрационному и акустическому каналамЛГШ-403 обеспечивает защиту путем постановки широкополосной виброакустической шумовой помехи на потенциально опасные конструкции помещений Кроме того, предусмотрена возможность установки акустического излучателя для защиты воздуховодов и вентиляционных шахтВ статье рассматриваются характерные особенности естественных каналов утечки речи, списываются методы и аппаратура активной виброакустической защиты помещенийДостаточно высокие акустические сопротивления строительных конструкций служат причиной возникновения и распространения так называемых структурных помех (уличных шумов, шагов, ударов дверей и тп) Уровень структурных помех, интенсивность которых уменьшается с увеличением частоты, а спектр близок спектру вибраций, и степень звукоизоляции помещений являются основными факторами, определяющими возможность прослушивания речи по акустическому (воздушному и вибрационному) каналам2 Способы и аппаратура активной защиты помещений от утечки речевой информацииВиброакустический канал утечки образуют: источники конфиденциальной информации (люди, технические устройства), среда распространения (воздух, ограждающие конструкции помещений, трубопроводы), средства съема (микрофоны, стетоскопы)Для защиты помещений применяют генераторы белого или розового шума и системы вибрационного зашумления, укомплектованные, как правило, электромагнитными и пьезоэлектрическими вибропреобразователямиВ большинстве случаев для активной защиты воздушных каналов используют системы виброзашумления, к выходам которых подключают громкоговорители

87 Способы и средства защиты телефонных каналов связи

При защите телефонных аппаратов и телефонных линий необходимо учитывать несколько аспектов:Для защиты телефонного аппарата от утечки акустической (речевой) информации по электроакустическому каналу используются как пассивные, так и активные методы и средстваК наиболее широко применяемым пассивным методам защиты относятся [12]:Диодные ограничители включаются последовательно в линию звонка (см рис 1 б) или непосредственно в каждую из телефонных линий (см рис 2) [2, 3, 5, 12]Простейшим фильтром является конденсатор, устанавливаемый в звонковую цепь телефонных аппаратов с электромеханическим звонком и в микрофонную цепь всех аппаратов (см рис 1, б и в) [2, 3, 5, 12] Емкость конденсаторов выбирается такой величины, чтобы зашунтировать зондирующие сигналы высокочастотного навязывания и не оказывать существенного влияния на полезные сигналы Обычно для установки в звонковую цепь используются конденсаторы, емкостью 1 мкФ, а для установки в микрофонную цепь - 0,01 мкФ [3]Для защиты телефонных аппаратов, как правило, используются устройства, сочетающие фильтр и ограничитель К ним относятся: устройства типа "Экран", "Гранит-8", "Корунд", "Грань-300" и др (см рис 2) [3]Отключение телефонных аппаратов от линииСамый простой способ реализации этого метода защиты заключается в установке в корпусе телефонного аппарата или телефонной линии специального выключателя, включаемого и выключаемого вручную Более удобным в эксплуатации является установка в телефонной линии специального устройства защиты, автоматически (без участия оператора) отключающего телефонный аппарат от линии при положенной телефонной трубке К типовым устройствам, реализующим данный метод защиты, относится изделие "Барьер- М1" В эго состав входят [13]:схема защиты телефонного аппарата от воздействия высоковольтных импульсовАктивные методы защиты от утечки информации по электроакустическому каналу предусматривают линейное зашумление телефонных линий Шумовой сигнал подается в линию в режиме, когда телефонный аппарат не используется (трубка положена) При снятии трубки телефонного аппарата подача в линию шумового сигнала прекращается

88 Методы и средства контроля эффективности технической защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами

 Контроль состояния ТЗИ включает:- технический контроль эффективности ТЗИ – контроль эффективности ТЗИ, проводимый с использованием технических средств контроля В зависимости от целей и задач контроля, а также особенностей проверяемых объектов технический контроль эффективности ТЗИ может быть:- комплексным, когда проводится проверка организации и состояния ТЗИ от утечки по всем возможным техническим каналам, характерным для контролируемого технического средства (объекта информатизации), от несанкционированного доступа к информации или специальных воздействий на нее; В зависимости от конкретных условий проведения технического контроля контроль эффективности может осуществляться следующими методами:- инструментальным методом, когда в ходе контроля используются технические измерительные средства и моделируются реальные условия работы технического средства разведки;- инструментально-расчетным методом, когда измерения проводятся в непосредственной близости от объекта контроля, а затем  результаты измерений пересчитываются к месту (условиям) предполагаемого места нахождения  технического средства разведки;- расчетным методом, когда эффективность ТЗИ оценивается путем расчета, исходя из реальных условий размещения и возможностей технического средства разведки и известных характеристик объекта контроляСущество мероприятий технического контроля состоит в осуществлении инструментальных (инструментально-расчетных) проверок эффективности защиты информации от утечки по техническим каналам, возникающим за счет:ГОСТ 29339-92 Информационная технология Защита информации от утечки за счет побочных электромагнитных излучений и наводок при ее обработке средствами вычислительной техники Общие технические требования;         Акт проверки состояния ТЗИ должен содержать следующие разделы:1 Общие сведения об объекте контроля;1216 Термины и определения; - средства вычислительной техники Защита от несанкционированного доступа к информации23 Постановку задач по комплексной2 защите информации, обрабатываемой автоматизированными системами, а также контроль за состоянием и развитием этого направления работ осуществляет Гостехкомиссия России

89 Оценка защищенности средств вычислительной техники от утечки за счет ПЭМИН

«Программное средство расчета показателей защищенности информации от утечки за счет ПЭМИН по результатам специальных исследований и оценки защищенности (эффективности защиты) информации, обрабатываемой средствами вычислительной техники, от утечки за счет ПЭМИН» («ПЭМИН ‑ 2018»)«ПЭМИН-2018» является наследованием средства контроля защищенности информации «ПЭМИН-2005» и соответствует требованиям, установленным в следующих документах:В работе приведён подход к оценке защищённости СВТ путём математического моделирования распространения электромагнитных волн от СВТАннотация В работе приведён подход к оценке защищённости СВТ путём математического моделирования распространения электромагнитных волн от СВТКлючевые слова: ПЭМИН, оценка защищённости, технические каналы утечки информации1 Оценка защищённости по каналу ПЭМИНПрактически все методики сводятся к разделению канала ПЭМИН на три зоны: ближнюю, промежуточную и дальнюю Они исходят из аппроксимации зависимостей уровня информативного сигнала от расстояния зависимостями 1/г, 1/г2 и 1/г3 и «стыковки» этих зависимостей на границах соответствующих зон Современный уровень развития вычислительной техники позволяет производить более точное моделирование канала ПЭМИНЛС Носов Оценка защищённостиПараметры электрического диполя, стоящие перед корнем в уравнениях для Ет и Нт, могут быть определены из измерений электрической и магнитной составляющей электромагнитного поля канала ПЭМИН Таким образом, оценка защищённости СВТ по каналу ПЭМИН может быть сведена к численному решению уравнений вида Ет — Еп и Нт — Нп, где величины Еп и Нп определяются нормативно-методическими документами из соотношения «сигнал/шум» [1]В работе предложен подход к оценке защищённости СВТ по каналу ПЭМИН путём численного решения уравнений для электромагнитных волн  
    Аппаратно - программный комплекс «Легенда-20» предназначен для проведения специальных исследований по каналу ПЭМИН технических средств обработки информации  
   
   Расчетная программа СПО «Легенда-18Р» (БЮЛИ

90 Средства измерения побочных электромагнитных излучений и наводок СВТ

﻿СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДОВ И СРЕДСТВКомплекс  «Легенда-05М» предназначен для проведения специальных исследований на побочные электромагнитные излучения и наводки (ПЭМИН) технических средств обработки информации Комплекс  создается на базе современных приборов ведущих производителей радиоизмерительной аппаратуры: «Agilent Technologies» (США), «Rohde Schwarz» (Германия) Комплекс  работает под управлением специального программного обеспечения, разработанного на основании действующих нормативно-методических документов ФСТЭК России Комплекс  сертифицирован по требованиям безопасности информации в системе сертификации ФСТЭК России )Описание актуально на: 29042012 Для уточнения технических характеристик «Комплекс для проведения специальных исследований на побочные электромагнитные излучения и наводки (ПЭМИН) "Легенда-05М"», а также для получения информации по наличию и условиям поставки Вы можете заполнить форму запроса ниже Внимание! Поставка оборудования осуществляется только юридическим лицами и только по безналичному расчёту Для уточнения технических характеристик «Комплекс для проведения специальных исследований на побочные электромагнитные излучения и наводки (ПЭМИН) "Легенда-05М"», а также для получения информации по наличию и условиям поставки Вы можете заполнить форму запроса ниже Внимание! Поставка оборудования осуществляется только юридическим лицами и только по безналичному расчёту Для уточнения технических характеристик «Комплекс для проведения специальных исследований на побочные электромагнитные излучения и наводки (ПЭМИН) "Легенда-05М"», а также для получения информации по наличию и условиям поставки Вы можете заполнить форму запроса ниже  
    Аппаратно - программный комплекс «Легенда-20» предназначен для проведения специальных исследований по каналу ПЭМИН технических средств обработки информации  
   
   Расчетная программа СПО «Легенда-18Р» (БЮЛИ  
   
 Специальное программное обеспечение «Легенда-18Р»  
   
 Специальное программное обеспечение «Легенда-20Упс»

91 Методы и средства контроля эффективности защиты выделенных помещений от утечки речевой информации по техническим каналам

В статье обоснованы показатели и критерии оценки эффективности защиты выделенных помещений от утечки речевой информации по техническим каналам Приведена методика инструментально-расчетного метода контроля эффективности защиты выделенных помещений от утечки речевой информации по техническим каналам Особенностью акустической (речевой) разведки является то, что анализ перехваченной с помощью средств разведки информации производит человек Поэтому в качестве показателя оценки эффективности защиты выделенных (защищаемых) помещений от утечки речевой информации используется словесная разборчивость речи Wс, под которой понимается относительное количество (в процентах) правильно понятых человеком слов из перехваченного разговораПоказатель словесной разборчивости речи используется для оценки эффективности защищенности помещений от утечки речевой информации по акустическому и виброакустическому каналам Наиболее целесообразно для оценки разборчивости речи использовать инструментально-расчетный метод, основанный на результатах экспериментальных исследований, проведенных НБ Покровским, описанным в книге "Расчет и измерение разборчивости речи" Для оценки разборчивости речи необходимо измерить уровни скрываемого речевого сигнала и шума (помехи) в месте возможного размещения приемных датчиков аппаратуры акустической разведки или в месте возможного прослушивания речи без применения технических средствСовременная аппаратура способна излучать контрольный сигнал одновременно во всех пяти октавных полосах С учетом того, что контроль защищенности требует множественных замеров, это сильно экономит общее время проведения оценки защищенностиКонтрольными точками установки акустического датчика (измерительного микрофона) являются места возможного размещения аппаратуры речевой разведки (стоянки автомобилей, автобусные остановки, скамейки для отдыха, окна близлежащих зданий и тп) При невозможности установки измерительного микрофона в реальных местах возможного расположения аппаратуры речевой разведки контрольные точки размещают на границе контролируемой (охраняемой) зоны При этом в оформлении результатов контроля об этом делается оговорка

92 Оценка защищенности выделенных помещений от утечки речевой информации

Метод оценки защищенности от утечки речевой конфиденциальной информации по акустическому каналу заключается в определении коэффициентов звукоизоляции его ограждающих конструкций (стены, пол, потолок, окна, двери и тп) в октавных полосах частот со среднегеометрическими частотами в соответствии с таблицей 52 и последующим сопоставлением полученных коэффициентов с их нормативными значениямиИнструментально-расчетная оценка защищенности помещения от утечки речевой конфиденциальной информации по акустическому (виброакустическому) каналуПодобная оценка защищенности помещения проводится при аттестации помещения и на соответствие требованиям защищенности при плановом периодическом контроле защищенности помещения, в тч после осуществления их ремонта и реконструкцииБ Метод оценки защищенностиМетод оценки защищенности от утечки речевой конфиденциальной информации по акустическому (виброакустическому) каналу заключается в определении коэффициентов звукоизоляции его ограждающих конструкций (стены, пол, потолок, окна, двери и тп) в октавных полосах частот со среднегеометрическими частотами 250, 500,1000,2000,4000, 8000 Гц и последующим сопоставлением полученных коэффициентов с их нормативными значениями В качестве тест-сигнала используются гармонические (тональные) частоты, соответствующие среднегеометрическим частотам октавных полосПри оценке защищенности помещений от утечки речевой информации по акустическому каналу для каждой ограждающей конструкции (ОК) выбирается не менее 3-х контрольных точек (КТ) в местах наиболее опасных с точки зрения перехвата речевой информацииобеспечивающих защищенность помещения от утечки речевой информации в зависимости от условий расположения приведены в таблице 52Место возможного перехвата речевой конфиденциальной информации из ЗПСмежные помещения1п), особенностей смежных помещений, прилегающих к ЗП- для ОК - пол или потолок АИ размещается в центре помещения на высоте 1-1,5м от пола Ось апертуры АИ направляется соответственно в сторону пола и потолка по нормали к его поверхности

93 Средства измерения акустических и вибрационных сигналов и шумов

Такие звуки принято называть шумом Четкой границы между звуками и шумом не существует Более того, иногда приходится выделять из последнего, так называемую тональную компоненту, которая  может оказаться даже  более раздражающей для человеческой психики, чем обычный шум Некоторые диссонансные аккорды воспринимаются любителями музыкального модерна как звуки, а его противниками — как раздражающий шум, и это при том, что и те и другие воспринимают звук с помощью одних и, тех же анализаторовАкустические сигналы встречаются нам даже дома на каждом шагу Это и шумящая стиральная машина, и даже вполне себе «бесшумный» холодильник иногда дает о себе знать, хотя, конечно, его не сравнить со старыми холодильниками из СССР типа «Саратов» Последним был присущ еще один вид шума, который называется грохот И еще один вид вибраций, который можно назвать маленьким землетрясением Дома необходимость анализировать шумовые аномалии у мотоцикла, или мотора катера, или  движущихся механизмов автомобиля диктуется соображениями экономии и безопасности, для этого можно воспользоваться анализатором шумов типа SonoscoutЧувствительность органа слуха человека к звукам различной частоты не одинакова Так называемые инфразвуковые колебания (ниже 15-20 Гц ) вообще не воспринимаются как звуки В области спектра 20-50 Гц чувствительность органа слуха хотя и отлична от нуля, но для некоторых задач не является достаточной, например для восприятия акустических сигналов сердца В этой области ухо в сочетании с мозгом не является качественным анализатором-инструментом для задач шумовых сигналов и вибраций в кардиофонии С повышением частоты до нескольких килогерц, (полоса охватывает практически все звуки сердца) чувствительность нашего анализатора шума существенно увеличивается с ростом частоты Эти шумомеры с функцией анализа результатов измерения являются удобной и компактной технологической платформой для поддерживающих ее программных приложений обработки результатов испытаний, встроенных в компактный и надежный высокоточный инструмент

94 Методы и средства выявления электронных устройств негласного получения информации

11(1) Осуществление лицензируемой деятельности иностранными юридическими лицами не допускаетсяа) выполнение работ по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях;б) выполнение работ по выявлению электронных устройств, предназначенных для негласного получения информации, в технических средствах4 Лицензирование деятельности, определенной настоящим Положением, осуществляется Федеральной службой безопасности Российской Федерации (далее - лицензирующий орган)5 Лицензионными требованиями при осуществлении лицензируемой деятельности являются:б) выполнение соискателем лицензии (лицензиатом) при осуществлении лицензируемой деятельности требований по обеспечению информационной безопасности, устанавливаемых в соответствии со статьями 112 и 13 Федерального закона "О федеральной службе безопасности";д) наличие у соискателя лицензии (лицензиата) лицензии на выполнение работ с использованием источников ионизирующего излучения (генерирующих) (за исключением случая, если эти источники используются в медицинской деятельности);руководитель и (или) лицо, уполномоченное руководить работами в рамках лицензируемой деятельности, имеющие высшее профессиональное (техническое) образование, а также профессиональную подготовку и (или) стаж работы не менее 5 лет в области лицензируемой деятельности;инженерно-технический работник (минимум 1 человек), имеющий высшее или среднее профессиональное (техническое) образование, а также профессиональную подготовку или стаж работы не менее 3 лет в области лицензируемой деятельности;6а) копии правоустанавливающих документов на помещения, здания, сооружения и иные объекты по месту осуществления лицензируемой деятельности, права на которые не зарегистрированы в Едином государственном реестре прав на недвижимое имущество и сделок с ним;л) сведения о документе, подтверждающем наличие лицензии на выполнение работ с использованием источников ионизирующего излучения (генерирующих) (за исключением случая, если эти источники используются в медицинской деятельности)

95 Методы и средства выявления электронных устройств негласного получения информации

11(1) Осуществление лицензируемой деятельности иностранными юридическими лицами не допускаетсяа) выполнение работ по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях;б) выполнение работ по выявлению электронных устройств, предназначенных для негласного получения информации, в технических средствах4 Лицензирование деятельности, определенной настоящим Положением, осуществляется Федеральной службой безопасности Российской Федерации (далее - лицензирующий орган)5 Лицензионными требованиями при осуществлении лицензируемой деятельности являются:б) выполнение соискателем лицензии (лицензиатом) при осуществлении лицензируемой деятельности требований по обеспечению информационной безопасности, устанавливаемых в соответствии со статьями 112 и 13 Федерального закона "О федеральной службе безопасности";д) наличие у соискателя лицензии (лицензиата) лицензии на выполнение работ с использованием источников ионизирующего излучения (генерирующих) (за исключением случая, если эти источники используются в медицинской деятельности);руководитель и (или) лицо, уполномоченное руководить работами в рамках лицензируемой деятельности, имеющие высшее профессиональное (техническое) образование, а также профессиональную подготовку и (или) стаж работы не менее 5 лет в области лицензируемой деятельности;инженерно-технический работник (минимум 1 человек), имеющий высшее или среднее профессиональное (техническое) образование, а также профессиональную подготовку или стаж работы не менее 3 лет в области лицензируемой деятельности;6а) копии правоустанавливающих документов на помещения, здания, сооружения и иные объекты по месту осуществления лицензируемой деятельности, права на которые не зарегистрированы в Едином государственном реестре прав на недвижимое имущество и сделок с ним;л) сведения о документе, подтверждающем наличие лицензии на выполнение работ с использованием источников ионизирующего излучения (генерирующих) (за исключением случая, если эти источники используются в медицинской деятельности)

96 Порядок проведения специальный обследований и исследований

24 декабря 2021(В редакции федеральных законов от 23062014 № 160-ФЗ, от 13072015 № 216-ФЗ, от 01Статья 1 Предмет регулирования настоящего Федерального закона 2) проводить внеплановую специальную оценку условий труда в порядке, установленном настоящим Федеральным законом;3) требовать от организации, проводящей специальную оценку условий труда, документы, подтверждающие ее соответствие требованиям, установленным статьей 19 настоящего Федерального закона;4) обжаловать в порядке, установленном статьей 26 настоящего Федерального закона, действия (бездействие) организации, проводящей специальную оценку условий труда; 1) обеспечить проведение специальной оценки условий труда, в том числе внеплановой специальной оценки условий труда, в случаях, установленных частью 1 статьи 17 настоящего Федерального закона;  3) обжаловать результаты проведения специальной оценки условий труда на его рабочем месте в соответствии со статьей 26 настоящего Федерального закона;1) отказаться в порядке, установленном настоящим Федеральным законом, от проведения специальной оценки условий труда, если при ее проведении возникла либо может возникнуть угроза жизни или здоровью работников такой организации;2) предоставлять по требованию работодателя документы, подтверждающие соответствие этой организации требованиям, установленным статьей 19 настоящего Федерального закона;б) отказа работодателя обеспечить условия, необходимые для проведения исследований (испытаний) и измерений идентифицированных вредных и (или) опасных производственных факторов, в соответствии с гражданско-правовым договором, указанным в части 2 статьи 8 настоящего Федерального закона;5) хранить коммерческую и иную охраняемую законом тайну, ставшую известной этой организации в связи с осуществлением деятельности в соответствии с настоящим Федеральным законом 5) организации в случаях, установленных законодательством Российской Федерации, обязательных предварительных (при поступлении на работу) и периодических (в течение трудовой деятельности) медицинских осмотров работников;

97 Организация технической защиты информации

Компания «Интегрус» оказывает услуги по настройке систем технической защиты информации предприятий, помогая предотвратить утечку данных и (или) несанкционированный доступ к сведениям компанииТехническая защита информации представляет собой целый комплекс работ: от оборудования помещений средствами ограничения доступа, шифрования данных, информирования коллектива и обнаружения предполагаемых каналов утечки до постоянного обновления средств и способов поддержания безопасностиТехническая защита направлена на повышение сохранности технологических данных, ноу-хау, информации из патентов, собственных наработок или приобретенных методик, лицензий Также методами и средствами технической защиты обеспечивается информационная безопасность сведений о финансовых операциях организации, кредитах, контрагентах, персональных данных (ПНд) сотрудников, руководства, клиентов и поставщиковДля построения эффективной технической защиты информации в информационных системах, базах данных, интернете, на предприятиях в целом все хранимые и обрабатываемые данные следует предварительно рассортировать по уровню ценности и их специфике Объектами системы технической защиты информации являются:Опасность для объектов технической защиты информации представляют:Сотрудники имеют доступ к объектам коммерческой информации и могут передать его посторонним (третьим) лицам Руководители – не обращают должного внимания на обеспечение безопасности сведений, полагая угрозы ложными (мнимыми) или несущественными Построение системы защиты данных начинается с разработки норм технического контроля защиты информацииТехническое обеспечение безопасности защиты конфиденциальной и коммерческой информации является совокупностью мероприятий, направленных на решение трех задач:Каналами, по которым «сливается» информация, часто являются неэкранированные проводка, контуры, приборы, подверженные воздействию электромагнитных полей Доступ к техническому каналу передачи информации означает ее беззащитность перед искажением, наведением помех, блокировкой либо несанкционированным использованием С целью получения информации злоумышленники могут использовать импульсопередающие устройства, выводящие из строя инженерно-техническую защиту

98 Порядок организации защиты информации от утечки по техническим каналам на объектах информатизации

К защищаемой информации относится информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации [3] Это, как правило, информация ограниченного доступа, содержащая сведения, отнесенные к государственной тайне, а также сведения конфиденциального характера09 № 333, “Положения о государственном лицензировании деятельности в области защиты информации”, утвержденного Постановлением Правительства РФ от 27 апреля 1994 г № 10, “Положения о лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации” утвержденного Постановлением Правительства РФ от 27 мая 2002 гРежим защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну (далее - конфиденциальной информации), устанавливается собственником информационных ресурсов или уполномоченным лицом в соответствии с законодательством Российской ФедерацииВ дальнейшем рассмотрим методические рекомендации по организации защиты конфиденциальной информации, собственником которой являются негосударственные предприятия (организации, фирмы)Мероприятия по защите конфиденциальной информации от утечки по техническим каналам (далее - технической защите информации) являются составной частью деятельности предприятий и осуществляются во взаимосвязи с другими мерами по обеспечению их информационной безопасностиТехнические мероприятия по защите информации от утечки по техническим каналам основываются на применении технических средств защиты и реализации специальных проектных и конструкторских решенийТехническая защита информации осуществляется подразделениями по защите информации (службами безопасности) или отдельными специалистами, назначаемыми руководителями организаций для проведения таких работ Для разработки мер по защите информации могут привлекаться сторонние организации, имеющие лицензии ФСТЭК или ФСБ России на право проведения соответствующих работ

99 Порядок организации и проведения аттестации объекта информатизации по требованиям безопасности информации

приказом ФСТЭК Россииот 29 апреля 2021 г N 775 N 79 (далее – орган по аттестации)6 N 1085 (Собрание законодательства Российской Федерации, 2004, N 34, ст 3541; 2020, N 35, ст 5554), национальных стандартов в области технической защиты информации;в) наименование и реквизиты документов ФСТЭК России, устанавливающих требования по защите информации, на соответствие которым проводится аттестация объекта информатизации; N 676 (Собрание законодательства Российской Федерации, 2015, N 28, ст 4241; 2020, N 42, ст 6615; 2021, N 23, ст 4079), модели угроз безопасности информации, технического задания на создание (развитие, модернизацию) объекта информатизации (только для государственных информационных систем); N 55 (зарегистрирован Минюстом России 11 мая 2018 г, регистрационный N 51063) (в случае наличия требования об обязательном применении сертифицированных средств защиты информации), или документов, подтверждающих проведение оценки соответствия средств защиты информации требованиям по безопасности информации в формах, отличных от сертификации;е) наименования и реквизиты документов ФСТЭК России, устанавливающих требования по защите информации, на соответствие которым проводилась аттестация объекта информатизации;2425 По согласованию с владельцем объекта информатизации работники ФСТЭК России (территориального органа ФСТЭК России) проводят контрольные испытания на объекте информатизации в соответствии с пунктами 15 и 16 настоящего Порядка26 Копия уведомления направляется владельцу объекта информатизации Орган по аттестации обязан устранить недостатки, выявленные ФСТЭК России по результатам оценки документов, в указанный в уведомлении срок и оформить аттестат соответствия Результаты проведенной оценки направляются ФСТЭК России (территориальным органом ФСТЭК России) владельцу объекта информатизации для устранения недостатков, выявленных органом по аттестации27 Орган по аттестации в течение 5 рабочих дней после подписания аттестата соответствия представляет в ФСТЭК России (территориальный орган ФСТЭК России) в электронном виде копии следующих документов: