Министерство образования и науки РФ
Федеральное государственное бюджетное образовательное учреждение высшего образования
АМУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
(ФГБОУ ВО «АмГУ»)

УПРАВЛЕНИЕ СРЕДСТВАМИ ЗАЩИТЫ ИНФОРМАЦИИ

сборник учебно-методических материалов для направления подготовки
10.03.01 Информационная безопасность

Благовещенск, 2019

Печатается по решению
редакционно-издательского совета
факультета математики и информатики
Амурского государственного
Университета

Составитель: Баранов А.А.

Управление средствами защиты информации: сборник учебно-методических материалов для направления подготовки 10.03.01 Информационная безопасность – Благовещенск: Амурский гос. ун-т, 2019.

Содержание

Краткое изложение лекционного материала.

Тема 1. Централизованное управление средствами защиты информации от несанкционированного доступа в локальной сети.

Цель лекции. Рассмотреть основные принципы и средства защиты информации.

План

1. Принципы построения средств защиты информации.
2. Основные механизмы защиты; аппаратные средства.
3. Конфигурирование; аудит; мониторинг и оперативное управление; полномочное управление доступом и контроль печати.

Краткое содержание

1.Простота механизма защиты. Этот принцип общеизвестен, но не всегда глубоко осознается. Действительно, некоторые ошибки, не выявленные при проектировании и эксплуатации, позволяют обнаружить неучтенные пути доступа. Необходимо тщательное тестирование программного обеспечения или аппаратных средств защиты, однако на практике такая проверка возможна только для простых и компактных схем.

2.В нормальных условиях доступ к механизму защиты должен отсутствовать

для работы системы необходимо, чтобы выполнялись определенные условия, при которых доступ к механизму защиты становится невозможным. Кроме того, считается, что запрет доступа при отсутствии особых указаний обеспечивает высокую степень надежности механизма защиты. Ошибка в определении полномочий пользователя в системе защиты, основанной на использовании разрешений, приводит к расширению сферы запретов. Эту ошибку легче обнаружить и она не разрушит общего статуса защиты.

3.Все возможные каналы утечки должны быть перекрыты. Этот принцип предпола-

гает проверку полномочий любого обращения к любому объекту и является основой системы защиты. Защита управления доступом с учетом этого принципа должна решаться на общесистемном уровне. При этом следует учитывать такие режимы работы как: запуск, восстановление после сбоев, выключение и профилактическое обслуживание. Необходимо обеспечить надежное определение источника любого обращения к данным.

4.Механизм защиты можно не засекречивать. Не имеет смысла засекречивать дета-

ли реализации систем защиты, предназначенной для широкого использования. Эффективность защиты не должна зависеть от того, насколько опытны потенциальные нарушители. Открытость механизма защиты позволяет при необходимости сделать его предметом обсуждения среди специалистов, не затрагивая при этом интересов пользователей.

5.**Разрешение полномочий**. Этот принцип заключается в применении нескольких ключей защиты. Наличие нескольких ключей защиты в АС удобно в тех условиях, когда право на доступ определяется выполнением ряда условий.

6.**Минимальные полномочия**. Для любой программы и любого пользователя должен быть определен минимальный круг полномочий, необходимых для выполнения порученной работы. Вследствие этого в значительной мере уменьшается ущерб, причиняемый при сбоях и случайных нарушениях.

7.Максимальная обоснованность механизма защиты. В целях исключения обмена информацией между пользователями рекомендуется при проектировании схем защиты сводить к минимуму число общих для нескольких пользователей параметров и характеристик механизма защиты.

8.**Психологическая привлекательность**. Система защиты должна быть простой в эксплуатации. Естественно, чем точнее совпадает представление пользователя о системе защиты с ее фактическими возможностями, тем меньше ошибок возникает в процессе применения.

Тема 2. Централизованная инвентаризация ресурсов локальной сети. Удалённый контроль работоспособности средств защиты информации на рабочих станциях.

Цель лекции. Рассмотреть основные методы и средства защиты информации**.**

План

1. Основы проведения инвентаризации ресурсов в локальной сети.
2. Подготовка к инспекциям; инспекции компьютеров; получение отчетов с результатами инспектирования.
3. Удалённый контроль работоспособности средств защиты информации на рабочих станциях.

Краткое содержание

Инвентаризация информационных ресурсов проводится для того, чтобы предоставить им должный уровень защиты.

Цели:

– ведение учета ресурсов, обеспечение достаточной уверенности их защиты;

– идентификация владельцев, распределение их ответственности, связанной с управлением информационной безопасности;

– идентификация ценности для того, чтобы выстроить мероприятия для управления рисками;

– другие цели, в том числе обеспечение безопасности трудящихся предприятия, их страхования и различные решения финансового плана.

Общие правила проведения инвентаризации

В Приказе Председателя правления устанавливается список ресурсов, которые подлежат информационной инвентаризации.

Те должностные лица, которые отвечают за наличие информационной безопасности, проверяют наличие ресурсов.

До того, как начинается проверка, комиссия должна получить такие документы:

– акты о том, что перемещались устройства, в том числе о списании и вводе в эксплуатацию, о перемещении на ремонт;

– карточки, описывающие рабочие места.

Все полученные базы данных должны сохраняться в двух экземплярах.

Фактическое наличие ресурсов можно определить только с помощью подсчетов, обмеров и обязательного взвешивания.

Процесс описи сопровождается обязательным использованием средства компьютерной техники.

Полученные результаты подписывают все члены службы, отвечающей за опись.

Правила проведения инвентаризации отдельных видов ресурсов

К системе информационных ресурсов относят:

– базы и файлы данных;
– системные документы;
– различные учебные данные и руководства для пользователя;
– всевозможные операционные процедуры;
– планы, обеспечивающие бесперебойную работу предприятия;
– процедуры, которые позволяют переходить в аварийный режим.

К категории, которая включает в себя все виды программных ресурсов, относят:

– системное и прикладное ПО (программное обеспечение);
– инструменты и утилиты.

К категории, которая включает в себя все виды физических ресурсов, относят:

– компьютерные, коммуникационные средства;
– диски, съемные носители данных;
– другие носители;
– оборудование рабочих мест и само помещение.

К категории, которая включает в себя все виды сервисов, относят:

– отопление, освещение, вентиляция, кондиционирование;
– вычислительные/телекоммуникационные сервисы.

Порядок оформления результатов инвентаризации

По результатам информационной инвентаризации составляются специальные описи, при этом для каждой категории отдельно.

После того, как они будут оформлены, составляется акт о том, что проведены работы.

Положение об инвентаризации ресурсов информационной системы компании

Во время инвентаризации информационной системы учитывают следующие факторы:

– инвентаризация информационных ресурсов должна быть простой, доступной и максимально полной, чтобы благодаря ней можно было полностью обеспечить максимальную степень защиты информационных ресурсов предприятия;
– список ресурсов пригодится для различных производственных целей, например, для обеспечения техники безопасности, а также для страхования;
– данная деятельность охватывает все ресурсы информации, в том числе и на реализацию работы каждой информационной системы;
– все ресурсы должны быть идентифицированы, а владельцы и категории критичности – согласованы.

Пример инвентаризации ресурсов в компании

Для каждого предприятия предусматривается несколько категорий ресурсов: информационные, программные, физические и сервисы. К первой относятся базы и файлы данных, процедуры, позволяющие работать бесперебойно или в автономном режиме, учебные пособия и руководства, различная системная документация. Вторая категория включает прикладное/системное ПО, различные программы и инструментальные средства. Физические ресурсы включают в себя компьютеры, комплектующие, носители данных, техническое оборудование, мебельные элементы и само помещение. К сервисам относятся вычислительные, телекоммуникационные, другие технические ресурсы.

Принципы и направления инвентаризации информационных систем

Стоит отметить, что для инвентаризации информационных ресурсов существует несколько основополагающих принципов. В первую очередь это однообразный подход ко всем видам проверок, во-вторых, это критический анализ и объективный подход ко всем предстоящим процедурам. Кроме того, обязательно практикуется многоуровневый подход, при этом сначала выделяются приоритетные направления. Также существует такой принцип, как сопряжение, при котором узнают, откуда поступают данные и куда они уходят. Контролируют проведение инвентаризации сразу несколько сторон, среди которых есть внешний аудитор, специальные фирмы и руководство предприятия.

Что касается направлений, то здесь также можно выделить несколько основных сфер, в соответствии с которыми осуществляются основные задачи. Если это физическая область, то имеют в виду расположение компонентов информационной системы и их схемы. К технологической области относят описание программного обеспечения, всех аппаратных средств, алгоритмы, в соответствии с которыми работает оборудование и соответствующие схемы сети.

Для функциональной сферы описываются задачи, которые выполняются для каждого элемента ИС отдельно. Организационное направление подразумевает под собой основные обязанности и рекомендации, которые выполняют пользователи и администраторы. Нормативная сфера представлена в виде документов, которые служат основой для осуществления всей работы системы. Информационная область дает возможность описать все базы данных, владельцев и доступ к получению такой информации.

Инвентаризация элементов информационной системы

На первом этапе специалист, работающий в службе по информационной безопасности, составляет перечень тех объектов и систем, а также субъектов, которые подлежат анализу. При этом он может заручиться поддержкой соответствующих служб и подразделений. Далее в такой перечень вносят первичные признаки и свойства таких объектов для того, чтобы их можно было описать с точки зрения информационной безопасности. Затем специалист проводит работу с различными пользователями, системами, администраторами, если они имеются на предприятии. С их помощью уточняются нюансы и дополнительные сведения по исследуемым объектам и субъектам. Причем действуют пользователи и администраторы в строго заданных рамках, установленных специалистом. Извлечением необходимых данных специалист занимается самостоятельно. Основой служат ранее полученные сведения и описания работы.

Существует определенная схема обследования, которая практически для всех компаний представлена в едином образце с корректировкой на направление деятельности организации. Сначала проводится знакомство со всей системой, визуально осматриваются все имеющиеся объекты, далее проводится интервьюирование менеджеров и администраторов о том, как функционирует вся система в общем. Затем специалист начинает знакомиться со всей необходимой документацией, которая присутствует в сфере информационной безопасности. После этого описывается вся система, и предоставляются уточнения такого описания.

Служба защиты информации: первые шаги

Стоит отметить, что информационная безопасность представляет собой целый комплекс мер, которые не могут быть более и менее важными. Такие меры защиты необходимо соблюдать в любой из точек сети, а также при обработке информации внешними субъектами. Компьютер отдельного пользователя, внешние носители, целый сервер, которой управляет всей сетью.

На 100% обеспечить защиту невозможно. Но при этом нужно понимать, что слишком сложная защищенность всей системы ведет к дополнительным сложностям в работе и делает ее более уязвимой. Например, при работе в 1С пользователь каждый раз может забывать слишком сложный пароль, поэтому может приклеивать стикеры на монитор со всеми паролями. Именно поэтому доступ к системе 1С могут иметь все, кто видит этот стикер.

Сегодня существует огромное количество самых разнообразных программных средств, обеспечивающих надежную защиту системы. Это могут быть антивирусные средства, специальное программное обеспечение, брандмауэры и многое другое. Самым уязвимым фактором для всей системы безопасности является человек. Именно поэтому в компаниях часто создается целый отдел, который обеспечивает информационную безопасность.

Информационная безопасность как система

Система информационной безопасности предполагает наличие средств, которые защищают как от случайных внедрений, так и от действий злоумышленников. Она является эффективным инструментом, который защищает данные и обычных пользователей, и руководства организации. Особенно актуальной такая система является для защиты персональной информации в банковских учреждениях и в заведениях открытого типа: школа, ВУЗах и т. д.

Необходимо понимать, что для всех сфер организация системы безопасности основывается на одинаковых принципах, поэтому подход к ее реализации всегда одинаков с определенными корректирующими элементами по типу деятельности. Также стоит отметить, что она требует постоянной модернизации, отличается уязвимостью при наличии определенных проблем, поэтому своевременная инвентаризация дает возможность снизить риск уязвимости такой системы.

Чем же занимается служба информационной безопасности? Она формирует многофункциональную структуру, а также осуществляет все виды мероприятий, которые обеспечивают должную защиту данных на предприятии. При этом для большинства организаций проще пользоваться услугами сторонних структур, чем пользоваться услугами собственной службы.

Внутренняя безопасность: подводные камни практического применения

Обеспечение внутренней безопасности – это проблема, которая сегодня остается очень актуальной для многих компаний. Они страдают из-за того, что неправильно используют сетевые ресурсы, при этом происходит утечка данных, которая угрожает безопасности компании. Инсайдером может оказаться каждый. Это может быть и администратор, и тот, кто находится в руководстве. В то же время на сегодняшний день существует достаточно большое количество средств, которые позволяют обеспечить информ. безопасность.

Как же происходит процесс вмешательства ИБ в деятельность фирмы? Сначала ставится задача, которая подразумевает под собой создание системы защиты, обеспечивающей предупреждение утечки информации. Также требуется вводить режим коммерческой тайны, а после этого выявляются злоумышленники.

Стоит отметить, что для коммерческих структур классификация защищаемых объектов по категориям достаточно простая. Более сложные процессы присутствуют в государственных структурах. Итак, в такую классификацию входят:

– общедоступная (открытая) информация, при работе с которой отсутствуют какие-либо ограничения;

– чувствительная информация с ограниченным доступом;

– персональные данные, включающие в себя зарплатные ведомости, больничные листы, анкетные данные каждого сотрудника;

– конфиденциальная информация с ограничениями для каждого пользователя по уровню допусков.

Тема 3. Централизованная защита от вирусов в локальной сети.

Цель лекции. Определить основные угрозы безопасности персональных данных пути их реализации.

План

Управление серверами администрирования.

Управление группами администрирования;

Управление клиентскими компьютерами; работа с отчетами, статистикой.

Краткое содержание

Создание иерархии Серверов администрирования: добавление подчиненного Сервера администрирования

Подключение к Серверу администрирования и переключение между Серверами администрирования

Права доступа к Серверу администрирования и его объектам

Условия подключения к Серверу администрирования через интернет

Защищенное подключение к Серверу администрирования

Отключение от Сервера администрирования
Добавление Сервера администрирования в дерево консоли
Удаление Сервера администрирования из дерева консоли
Добавление виртуального Сервера администрирования в дерево консоли
Смена учетной записи службы Сервера администрирования. Утилита klsrvswch
Решение проблем с узлами Сервера администрирования
Просмотр и изменение параметров Сервера администрирования
Резервное копирование и восстановление параметров Сервера администрирования
Резервное копирование и восстановление данных Сервера администрирования
Избегание конфликтов между Серверами администрирования

Тема 4. Централизованный учет и управление программно аппаратными средствами защиты информации

Цель лекции. Рассмотреть основной механизм многоподьзовательских систем для обеспечения конфиденциальность и целостность объектов.

План

1. Назначение средств учета и управления аппаратными идентификаторами и носителями ключевой информации; возможности; архитектура; настройка;
2. Управление жизненным циклом средств аутентификации;
3. Аудит использования средств аутентификации.

Краткое содержание

С традиционной точки зрения средства управления доступом позволяют специфицировать и контролировать действия, которые субъекты (пользователи и процессы) могут выполнять над **объектами** (информацией и другими компьютерными ресурсами). В данном разделе речь идет о логическом управлении доступом, которое, в отличие от физического, реализуется программными средствами. Логическое управление доступом – это основной механизм многопользовательских систем, призванный обеспечить конфиденциальность и целостность объектов и, до некоторой степени, их доступность (путем запрещения обслуживания неавторизованных пользователей).

Рассмотрим формальную постановку задачи в традиционной трактовке. Имеется совокупность субъектов и набор объектов. Задача логического управления доступом состоит в том, чтобы для каждой пары "субъект-объект" определить множество допустимых операций (зависящее, быть может, от некоторых дополнительных условий) и контролировать выполнение установленного порядка.

Отношение "субъекты-объекты" можно представить в виде **матрицы доступа**, в строках которой перечислены субъекты, в столбцах – объекты, а в клетках, расположенных на пересечении строк и столбцов, записаны дополнительные условия (например, время и место действия) и разрешенные виды доступа.

Тема логического управления доступом – одна из сложнейших в области информационной безопасности. Дело в том, что само понятие объекта (а тем более видов доступа) меняется от сервиса к сервису. Для операционной системы к объектам относятся *файлы, устройства* и процессы. Применительно к файлам и устройствам обычно рассматриваются права на чтение, запись, выполнение (для программных файлов), иногда на удаление и добавление. Отдельным правом может быть возможность передачи полномочий доступа

другим субъектам (так называемое право владения). Процессы можно создавать и уничтожать. Современные операционные системы могут поддерживать и другие объекты.

Для систем управления реляционными базами данных объект – это база данных, таблица, представление, хранимая процедура. К таблицам применимы операции поиска, добавления, модификации и удаления данных, у других объектов иные виды доступа.

Разнообразие объектов и применимых к ним операций приводит к принципиальной децентрализации логического управления доступом. Каждый сервис должен сам решать, позволить ли конкретному субъекту ту или иную операцию. Теоретически это согласуется с современным объектно-ориентированным подходом, на практике же приводит к значительным трудностям. Главная проблема в том, что ко многим объектам можно получить доступ с помощью разных сервисов (возможно, при этом придется преодолеть некоторые технические трудности). Так, до реляционных таблиц можно добраться не только средствами СУБД, но и путем непосредственного *чтения файлов* или дисковых разделов, поддерживаемых операционной системой (разобравшись предварительно в *структуре хранения*объектов базы данных). В результате при задании матрицы доступа нужно принимать во внимание не только принцип распределения привилегий для каждого сервиса, но и существующие связи между сервисами (приходится заботиться о согласованности разных частей матрицы). Аналогичная трудность возникает при экспорте/импорте данных, когда информация о правах доступа, как правило, теряется (поскольку на новом сервисе она не имеет смысла). Следовательно, обмен данными между различными сервисами представляет особую опасность с точки зрения управления доступом, а при проектировании и реализации разнородной конфигурации необходимо позаботиться о согласованном распределении прав доступа субъектов к объектам и о минимизации числа способов экспорта/импорта данных.

При принятии решения о предоставлении доступа обычно анализируется следующая информация:

- идентификатор субъекта (идентификатор пользователя, сетевой адрес компьютера и т.п.). Подобные идентификаторы являются основой **произвольного (или дискреционного) управления доступом** ;
- атрибуты субъекта (*метка безопасности*, группа пользователя и т.п.). *Метки безопасности* – основа **принудительного (мандатного) управления доступом**.

Матрицу доступа, ввиду ее разреженности (большинство клеток – пустые), неразумно хранить в виде двухмерного массива. Обычно ее хранят по столбцам, то есть для каждого объекта поддерживается список "допущенных" субъектов вместе с их правами. Элементами списков могут быть имена групп и шаблоны субъектов, что служит большим подспорьем администратору. Некоторые проблемы возникают только при удалении субъекта, когда приходится удалять его имя из всех списков доступа; впрочем, эта операция производится не часто.

Списки доступа – исключительно гибкое средство. С их помощью легко выполнить требование о *гранулярности* прав с точностью до пользователя. Посредством списков несложно добавить права или явным образом запретить доступ (например, чтобы наказать нескольких членов группы пользователей). Безусловно, списки являются лучшим средством *произвольного управления доступом*.

Подавляющее большинство операционных систем и систем управления базами данных реализуют именно *произвольное управление доступом*. Основное достоинство произвольного управления – гибкость. Вообще говоря, для каждой пары "субъект-объект" можно независимо задавать права доступа (особенно легко это делать, если используются **списки управления доступом**). К сожалению, у "произвольного" подхода есть ряд недостатков. Рассредоточенность управления доступом ведет к тому, что доверенными должны быть многие пользователи, а не только системные операторы или администраторы. Из-за рассеянности или некомпетентности сотрудника, владеющего секретной инфор-

мацией, эту информацию могут узнать и все остальные пользователи. Следовательно, произвольность управления должна быть дополнена жестким контролем за реализацией избранной политики безопасности.

Второй недостаток, который представляется основным, состоит в том, что права доступа существуют отдельно от данных. Ничто не мешает пользователю, имеющему доступ к секретной информации, записать ее в доступный всем файл или заменить полезную утилиту ее "троянским" аналогом. Подобная "разделенность" прав и данных существенно осложняет проведение несколькими системами согласованной политики безопасности и, главное, делает практически невозможным эффективный контроль согласованности.

Возвращаясь к вопросу представления матрицы доступа, укажем, что для этого можно использовать также функциональный способ, когда матрицу не хранят в явном виде, а каждый раз вычисляют содержимое соответствующих клеток. Например, при принудительном управлении доступом применяется сравнение меток безопасности субъекта и объекта.

Удобной надстройкой над средствами логического управления доступом является **ограничивающий интерфейс**, когда пользователя лишают самой возможности попытаться совершить несанкционированные действия, включив в число видимых ему объектов только те, к которым он имеет доступ. Подобный подход обычно реализуют в рамках системы меню (пользователю показывают лишь допустимые варианты выбора) или посредством ограничивающих оболочек, таких как restricted shell в ОС Unix.

В заключение подчеркнем важность управления доступом не только на уровне операционной системы, но и в рамках других сервисов, входящих в состав современных приложений, а также, насколько это возможно, на "стыках" между сервисами. Здесь на первый план выходит существование единой политики безопасности организации, а также квалифицированное и согласованное системное администрирование.

Ролевое управление доступом

При большом количестве пользователей традиционные подсистемы управления доступом становятся крайне сложными для администрирования. Число связей в них пропорционально произведению количества пользователей на количество объектов. Необходимы решения в объектно-ориентированном стиле, способные эту сложность понизить.

Таким решением является **ролевое управление доступом** (РУД). Суть его в том, что между пользователями и их привилегиями появляются промежуточные сущности – роли. Для каждого пользователя одновременно могут быть активными несколько ролей, каждая из которых дает ему определенные права.

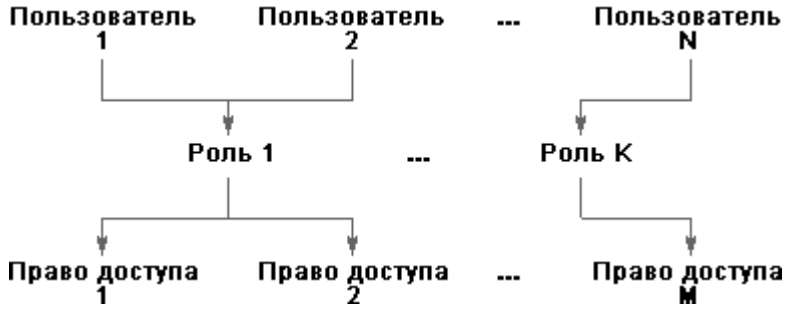

Рисунок – Пользователи, объекты и роли.

Ролевой доступ нейтрален по отношению к конкретным видам прав и способам их проверки; его можно рассматривать как объектно-ориентированный каркас, облегчающий администрирование, поскольку он позволяет сделать подсистему разграничения доступа управляемой при сколь угодно большом числе пользователей, прежде всего за счет установления между ролями связей, аналогичных наследованию в объектно-ориентированных системах. Кроме того, ролей должно быть значительно меньше, чем пользователей. В результате число администрируемых связей становится пропорциональным сумме (а не

произведению) количества пользователей и объектов, что по порядку величины уменьшить уже невозможно.

Ролевой доступ развивается более 10 лет (сама идея ролей, разумеется, значительно старше) как на уровне операционных систем, так и в рамках СУБД и других *информационных сервисов*. В частности, существуют реализации ролевого доступа для Web-серверов.

В 2001 году Национальный институт стандартов и технологий США предложил проект стандарта *ролевого управления доступом* , основные положения которого мы и рассмотрим.

Ролевое управление доступом оперирует следующими основными понятиями:

- **пользователь** (человек, интеллектуальный автономный агент и т.п.);
- **сеанс работы пользователя** ;
- **роль** (обычно определяется в соответствии с организационной структурой);
- **объект** (сущность, доступ к которой разграничивается; например, файл ОС или таблица СУБД);
- **операция** (зависит от объекта; для файлов ОС – чтение, запись, выполнение и т.п.; для таблиц СУБД – вставка, удаление и т.п., для прикладных объектов операции могут быть более сложными);
- право доступа (разрешение выполнять определенные операции над определенными объектами).

Ролям приписываются пользователи и права доступа ; можно считать, что они (роли) именуют отношения "многие ко многим" между пользователями и правами. Роли могут быть приписаны многим пользователям; один пользователь может быть приписан нескольким ролям. Во время сеанса работы пользователя активизируется подмножество ролей, которым он приписан, в результате чего он становится обладателем объединения прав, приписанных активным ролям. Одновременно пользователь может открыть несколько сеансов.

Между ролями может быть определено *отношение частичного порядка*, называемое наследованием. Если роль r2 является наследницей r1, то все права r1 приписываются r2, а все пользователи r2 приписываются r1. Очевидно, что **наследование ролей** соответствует наследованию классов в объектно-ориентированном программировании, только правам доступа соответствуют методы классов, а пользователям – объекты (экземпляры) классов.

Отношение наследования является иерархическим, причем права доступа и пользователи распространяются по уровням иерархии навстречу друг другу. В общем случае наследование является множественным, то есть у одной роли может быть несколько предшественниц (и, естественно, несколько наследниц, которых мы будем называть также преемницами).

Можно представить себе формирование **иерархии ролей**, начиная с минимума прав (и максимума пользователей), приписываемых роли "сотрудник", с постепенным уточнением состава пользователей и добавлением прав (роли "системный администратор", "бухгалтер" и т.п.), вплоть до роли "руководитель" (что, впрочем, не значит, что руководителю предоставляются неограниченные права; как и другим ролям, в соответствии с принципом **минимизации привилегий**, этой роли целесообразно разрешить только то, что необходимо для выполнения служебных обязанностей). Фрагмент подобной *иерархии ролей* показан на рис.

Рисунок – Фрагмент иерархии ролей.

Для реализации еще одного упоминавшегося ранее важного принципа информационной безопасности вводится понятие **разделения обязанностей**, причем в двух видах: статическом и динамическом.

Статическое разделение обязанностей налагает ограничения на **приписывание пользователей ролям**. В простейшем случае членство в некоторой роли запрещает приписывание пользователя определенному множеству других ролей. В общем случае данное ограничение задается как пара "множество ролей – число" (где множество состоит, по крайней мере, из двух ролей, а число должно быть больше 1), так что никакой пользователь не может быть приписан указанному (или большему) числу ролей из заданного множества. Например, может существовать пять бухгалтерских ролей, но политика безопасности допускает членство не более чем в двух таких ролях (здесь число=3).

При наличии наследования ролей ограничение приобретает несколько более сложный вид, но суть остается простой: при проверке членства в ролях нужно учитывать приписывание пользователей ролям-наследницам.

Динамическое разделение обязанностей отличается от статического только тем, что рассматриваются роли, одновременно активные (быть может, в разных сеансах) для данного пользователя (а не те, которым пользователь статически приписан). Например, один пользователь может играть роль и кассира, и контролера, но не одновременно; чтобы стать контролером, он должен сначала закрыть кассу. Тем самым реализуется так называемое **временное ограничение доверия**, являющееся аспектом *минимизации привилегий*.

Рассматриваемый проект стандарта содержит спецификации трех *категорий функций*, необходимых для администрирования РУД:

- **Административные функции** (создание и сопровождение ролей и других атрибутов ролевого доступа): создать/удалить роль/пользователя, приписать пользователя/право роли или ликвидировать существующую ассоциацию, создать/удалить *отношение наследования* между существующими ролями, создать новую роль и сделать ее наследницей/предшественницей существующей роли, создать/удалить ограничения для статического/динамического *разделения обязанностей*.
- **Вспомогательные функции** (обслуживание сеансов работы пользователей): открыть сеанс работы пользователя с активацией подразумеваемого набора ролей; активировать новую роль, деактивировать роль; проверить правомерность доступа.
- **Информационные функции** (получение сведений о текущей конфигурации с учетом отношения наследования). Здесь проводится разделение на обязательные и необязательные функции. К числу первых принадлежат получение списка пользователей, приписанных роли, и списка ролей, которым приписан пользователь.

Все остальные функции отнесены к разряду необязательных. Это получение информации о правах, приписанных роли, о правах заданного пользователя (которыми он обладает как член множества ролей), об активных в данный момент сеанса ролях и правах, об операциях, которые роль/пользователь правомочны совершить над заданным объектом, о статическом/динамическом разделении обязанностей.

Можно надеяться, что предлагаемый стандарт поможет сформировать единую терминологию и, что более важно, позволит оценивать РУД-продукты с единых позиций, по единой шкале.

Тема 5. Анализ нормативных требований по управлению средствами защиты информации.

Цель лекции. Анализ нормативных требований по управлению средствами защиты информации.

План

1. Анализ нормативных требований по управлению средствами защиты информации.

2. Анализ нормативных требований Федеральной службы по техническому и экспортному контролю (ФСТЭК) при обеспечении мер безопасности персональных данных, в государственных информационных системах.

3. Анализ требований безопасности к автоматизированным системам управления технологическими процессами

Краткое содержание

Федеральная служба по техническому и экспортному контролю (ФСТЭК) создана Указом Президента российской Федерации от 16 августа 2004 года № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю». Этим же Указом утверждено Положение о ФСТЭК, которое затем корректировалось Указами Президента от

22.03.2005 № 330, от 20.07.2005 № 846, от 30.11.2006 № 1321.

ФСТЭК, ее территориальные органы и подведомственные ей организации являются правопреемниками Государственной технической комиссии при Президенте Российской Федерации, созданной Указом Президента Российской Федерации от 5 января 1992 года № 9 «О создании государственной технической комиссии при Президенте Российской Федерации». Функции комиссии были уточнены Указом Президента от 19 февраля 1999 года № 212 "Вопросы Государственной технической комиссии при Президенте Российской Федерации".

ФСТЭК является федеральным органом исполнительной власти, осуществляющим реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности по вопросам:

1)обеспечения безопасности (некриптографическими методами) информации в системах информационной и телекоммуникационной инфраструктуры, оказывающих существенное влияние на безопасность государства в информационной сфере;

2)противодействия иностранным техническим разведкам на территории Российской Федерации;

3)обеспечения защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную тайну, иной информации с ограниченным доступом, предотвращения ее утечки по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию (носители информации) в целях

еедобывания, уничтожения, искажения и блокирования доступа к ней на территории Российской Федерации;

4)защиты информации при разработке, производстве, эксплуатации и утилизации неинформационных излучающих комплексов, систем и устройств;

159

5) осуществления экспортного контроля.

ФСТЭК России является федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности информации в ключевых системах информационной инфраструктуры, организует деятельность государственной системы противодействия техническим разведкам и технической защиты информации.

Руководство деятельностью ФСТЭК России осуществляет Президент Российской Федерации. ФСТЭК России подведомственна Министерству обороны России.

ФСТЭК осуществляет самостоятельно нормативно-правовоерегулирование вопросов в области обеспечения безопасности информации в ключевых системах информационной инфраструктуры, технической защиты информации.

ФСТЭК России в своей деятельности руководствуется Конституцией Российской Федерации, федеральными конституционными законами, федеральными законами, актами Президента Российской Федерации и Правительства Российской Федерации, международными договорами Российской Федерации, приказами и директивами Министра обороны Российской Федерации в части, касающейся ФСТЭК России, а также другими нормативными правовыми актами Российской Федерации, касающимися деятельности ФСТЭК России.

Нормативные правовые акты и методические документы, изданные по вопросам деятельности ФСТЭК России, обязательны для исполнения аппаратами федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, федеральными органами исполнительной власти, органами исполнительной власти субъектов Российской Федерации, органами местного самоуправления и организациями.

Деятельность ФСТЭК России обеспечивают Государственный научно-исследовательскийиспытательный институт проблем технической защиты информации ФСТЭК России (головная научная организация по проблемам защиты информации), а также другие подведомственные ФСТЭК России организации.

ФСТЭК вносит Президенту Российской Федерации, в Правительство Российской Федерации и Совет Безопасности Российской Федерации предложения по нормативно-правовомурегулированию в области обеспечения безопасности информации, контролирует эффективность защиты информации в ключевых системах информационной инфраструктуры, в информационных системах и объектах, на которых выполняются работы, связанные со сведениями, составляющими государственную и (или) служебную тайну.

ФСТЭК имеет право заслушивать на заседаниях коллегии должностных лиц, уполномоченных по вопросам обеспечения безопасности информации в ключевых системах информационной инфраструктуры и технической защиты информации.

ФСТЭК России осуществляет следующие полномочия:

1.Разрабатывает стратегию и определяет приоритетные направления деятельности по обеспечению безопасности информации.

2.Организует и проводит лицензирование деятельности по осуществлению мероприятий и (или) оказанию услуг в области технической защиты государственной тайны, по созданию средств защиты информации, содержащей сведения, составляющие государственную тайну, по технической защите конфиденциальной информации, по разработке и (или) производству средств защиты конфиденциальной информации.

3.Организует проведение работ сертификации средств технической защиты информации, обеспечения безопасности

Тема 6. Администрирование и управление средствами защиты информации от несанкционированного доступа.

Цель лекции. Рассмотреть основные методы управления средствами защиты от несанкционированного доступа

План

1. Администрирование и управление средствами защиты информации от несанкционированного доступа.
2. Модель безопасности белла-ЛаПадулы. Ролевая модель контроля доступа (RBAC).
3. Системы разграничения доступа
4. Понятие сервисов безопасности.

.

Краткое содержание

Выделяется три обобщенных механизма управления доступом к данным: идентификация пользователя, непосредственная (физическая) защита данных и поддержка прав доступа пользователя к данным с возможностью их передачи.

Идентификация пользователей определяет шкалу доступа к различным базам данных или частям баз данных (отношениям или атрибутам). Это, по существу, информационный табель о рангах. Физическая защита данных больше относится к организационным мероприятиям, хотя отдельные вопросы могут касаться непосредственно данных, например их кодирование. И, наконец, средства поддержки и передачи прав доступа должны строго задавать характер дифференцированного общения с данными.

Метод защиты при помощи программных паролей. Согласно этому методу, реализуемому программными средствами, процедура общения пользователя с ПК построена так, что запрещается доступ к операционной системе или определенным файлам до тех пор, пока не будет введен пароль. Пароль держится пользователем в тайне и периодически меняется, чтобы предотвратить несанкционированное его использование.

Метод паролей является самым простым и дешевым, однако не обеспечивает надежной защиты. Не секрет, что пароль можно подсмотреть или подобрать, используя метод проб и ошибок или специальные программы, и получить доступ к данным. Более того, основная уязвимость метода паролей заключается в том, что пользователи зачастую выбирают очень простые и легкие для запоминания (и тем самым для разгадывания) пароли, которые не меняются длительное время, а нередко остаются прежними и при смене пользователя. Несмотря на указанные недостатки, применение метода паролей во многих случаях следует считать рациональным даже при наличии других аппаратных и программных методов защиты. Обычно метод программных паролей сочетается с другими программными методами, определяющими ограничения по видам и объектам доступа.

Проблема защиты информации от несанкционированного доступа особо обострилась с широким распространением локальных и, особенно, глобальных компьютерных сетей. В связи с этим, помимо контроля доступа, необходимым элементом защиты информации в компьютерных сетях является разграничение полномочий пользователей.

В компьютерных сетях при организации контроля доступа и разграничения полномочий пользователей чаще всего используются встроенные средства сетевых операционных систем (ОС). Использование защищенных операционных систем является одним из важнейших условий построения современных информационных систем. Например, ОС UNIX позволяет владельцу файлов предоставлять права другим пользователям — только читать или записывать, для каждого из своих файлов. Наибольшее распространение в нашей стране получает ОС Windows NT, в которой появляется все больше возможностей для построения сети, действительно защищенной от НД к информации. ОС NetWare помимо стандартных средств ограничения доступа, таких как система паролей и разграничения полномочий, имеет ряд новых возможностей, обеспечивающих первый класс защиты данных, предусматривает возможность кодирования данных по принципу «открытого ключа» (алгоритм RSA) с формированием электронной подписи для передаваемых по сети пакетов.

В то же время в такой системе организации защиты все равно остается слабое место: уровень доступа и возможность входа в систему определяются паролем. Для исключения возможности неавторизованного входа в компьютерную сеть в последнее время ис-

пользуется комбинированный подход — пароль + идентификация пользователя по персональному «ключу». В качестве «ключа» может использоваться пластиковая карта (магнитная или со встроенной микросхемой — smart-card) или различные устройства для идентификации личности по биометрической информации — по радужной оболочке глаза или отпечатков пальцев, размерам кисти руки и т. д.

Пластиковые карточки с магнитной полосой можно легко подделать. Более высокую степень надежности обеспечивают смарт-карты — так называемые микропроцессорные карточки (МП-кар-точки). Их надежность обусловлена в первую очередь невозможностью копирования или подделки кустарным способом. Кроме того, при производстве карточек в каждую микросхему заносится уникальный код, который невозможно продублировать. При выдаче карточки пользователю на нее наносится один или несколько паролей, известных только ее владельцу. Для некоторых видов МП-карточек попытка несанкционированного использования заканчивается ее автоматическим «закрытием». Чтобы восстановить работоспособность такой карточки, ее необходимо предъявить в соответствующую инстанцию. Кроме того, технология МП-карто-чек обеспечивает шифрование записанных на ней данных в соответствии со стандартом DES. Установка специального считывающего устройства МП — карточек возможна не только на входе в помещения, где расположены компьютеры, но и непосредственно на рабочих станциях и серверах сети.

Этот подход значительно надежнее применения паролей, поскольку, если пароль подглядели, пользователь об этом может не знать, если же пропала карточка, можно принять меры немедленно.

Смарт-карты управления доступом позволяют реализовать, в частности, такие функции, как контроль входа, доступ к устройствам персонального компьютера, доступ к программам, файлам и командам. Кроме того, возможно также осуществление контрольных функций, в частности, регистрация попыток нарушения доступа к ресурсам, использования запрещенных утилит, программ, команд DOS.

По мере расширения деятельности предприятий, роста численности персонала и появления новых филиалов возникает необходимость доступа удаленных пользователей (или групп пользователей) к вычислительным и информационным ресурсам главного офиса компании. Чаще всего для организации удаленного доступа используются кабельные линии (обычные телефонные или выделенные) и радиоканалы. В связи с этим защита информации, передаваемой по каналам удаленного доступа, требует особого подхода.

В частности, в мостах и маршрутизаторах удаленного доступа применяется сегментация пакетов — их разделение и передача параллельно по двум линиям, — что делает невозможным «перехват» данных при незаконном подключении «хакера» к одной из линий. К тому же используемая при передаче данных процедура сжатия передаваемых пакетов гарантирует невозможность расшифровки «перехваченных» данных. Кроме того, мосты и маршрутизаторы удаленного доступа могут быть запрограммированы таким образом, что удаленные пользователи будут ограничены в доступе к отдельным ресурсам сети главного терминала.

Метод автоматического обратного вызова может обеспечивать более надежную защиту системы от несанкционированного доступа, чем простые программные пароли. В данном случае пользователю нет необходимости запоминать пароли и следить за соблюдением их секретности. Идея системы с обратным вызовом достаточно проста. Удаленные от центральной базы пользователи не могут непосредственно с ней обращаться. Вначале они получают доступ к специальной программе, которой сообщают соответствующие идентификационные коды. После этого разрывается связь и производится проверка идентификационных кодов. В случае если код, посланный по каналу связи, правильный, то производится обратный вызов пользователя с одновременной фиксацией даты, времени и номера телефона. К недостатку рассматриваемого метода следует отнести низкую скорость обмена — среднее время задержки может исчисляться десятками секунд.

Методические указания к практическим занятиям

Практическая работа 1.

Разграничение доступа к данным.

Цель занятия. Изучение основных понятий и определений, связанных с дисциплиной..

Задание

1. Разграничение доступа к устройствам.
2. Выполнить контроль печати конфиденциальных данных.
3. Построить глоссарий по теме

Контрольные вопросы

1. Что такое информационная безопасность?
2. Перечислить виды угроз.
3. Назвать методы защиты информации?
4. Раскрыть понятие компьютерное преступление.
5. Что такое конфиденциальность информации?
6. Что такое целостность данных?
7. Что такое доступность данных?
8. В каком случае информация считается защищенной?
9. Назвать источники информации, требующие защиты?
10. Что относится к способам получения доступа к информации?

Практическая работа 2.

Аудит событий информационной безопасности

Цель занятия. Научиться строить модели безопасности для различных предметных областей.

Задание

1. Аудит событий информационной безопасности СЗИ от НСД.
2. Работа со сведениями в журнале регистрации событий.
3. Теневое копирование.
4. Выполнить анализ основных видов моделей безопасности.
5. Решение ситуационных задач в группах по составлению неформальных политик безопасности для заданной автоматизированной системе.

Контрольные вопросы

1. Какие основные виды политики безопасности известны?
2. В чем суть дискреционной политики безопасности?
3. Какими условиями определяется мандатная политика безопасности?
4. Чем отличается политика безопасности информационных потоков от политики ролевого разграничения доступа?
5. Какова цель реализации политики изолированной программной среды?
6. Что такое матрица доступов?
7. Перечислить классические угрозы безопасности?
8. Как описываются информационные потоки по времени и по памяти?
9. Какие математические понятия используются в моделях безопасности?

10. Какая задача является алгоритмически разрешимой?

Практическая работа 3.

Оперативное управление защищаемыми рабочими станциями и мониторинг событий информационной безопасности

Цель занятия. Выявить проблемы, связанные с оперативным управлением защищаемых рабочих станций.

Задание

1. Рассмотреть теоретические вопросы оперативного управления рабочими станциями
2. Для банковской ИС решить задачу управления рабочими станциями.
3. Мониторинг событий информационной безопасности

Контрольные вопросы

1. Что такое разграничение доступа?
2. В чем суть ролевого управления?
3. Почему протоколирование и аудит относят к пассивным сервисам безопасности?
4. Какие функции выполняет экранирование как сервис безопасности?
5. Для каких целей используется туннелирование?

Практическая работа 4

Замкнутая программная среда и контроль потоков информации.

Цель занятия. Рассмотреть понятие замкнутая программная среда, проблемы и пути решения.

Задание

1. Концепция изолированной программной среды.
2. Домены безопасности.
3. Определить замкнутую программную среду для торговой организации, образовательного учреждения, медицинского учреждения.

Контрольные вопросы

1. Что такое замкнутая программная среда?
2. Что такое UEL-список?
3. Как настраивается замкнутая программная среда?
4. Какими сервисами обладает Операционная система специального назначения «Astra Linux Special Edition» РУСБ.10015-01 для отслеживания работы замкнутой программной среды.
5. Что такое мягкий режим замкнутой программной среды?
6. Чем отличается мягкий режим замкнутой программной среды от жесткого режима.

Практическая работа 5

Централизованная инвентаризация ресурсов локальной сети

Цель занятия. Рассмотреть проблемы инвентаризации ресурсов локальной сети

Задание.

1. Проведение инспекций и учет изменений конфигурации защищаемых рабочих станций.
2. Определить мероприятия для проведения инвентаризации рескрсов локальной сети.
3. Рассмотреть механизм функционирования вредоносного ПО.

Контрольные вопросы

1. Что такое компьютерный вирус? Какими свойствами обладают компьютерные вирусы?
2. По каким признакам классифицируют компьютерные вирусы? Перечислите типы вирусов.
3. Какие вирусы называются резидентными и в чем особенность таких вирусов?
4. Каковы отличия вирусов-репликаторов, стелс - вирусов, мутантов и «троянских» программ?
5. Опишите схему функционирования загрузочного вируса.
6. Опишите схему функционирования файлового вируса.
7. Опишите схему функционирования загрузочно-файловых вирусов.
8. Что такое полиморфный вирус? Почему этот тип вирусов считается наиболее опасным?

Практическая работа 6

Управление серверами администрирования Kaspersky Security Center.

Цель занятия. Рассмотреть процессы настройки средств антивирусной защиты Kaspersky Endpoint Security..

.

Задание

1. Изучение документа "Руководящий документ средства вычислительной техники защита от несанкционированного доступа к информации показатели защищенности от несанкционированного доступа к информации " (утв. Гостехкомиссией при президенте рф от 30.03.92)
2. В соответствии с руководящим документом выполнить классификацию средств вычислительной техники для медицинского учреждения.
3. Определить план проведения аудита событий в АС

Контрольные вопросы

1. Перечислить классы защищенности СВТ?
2. Назвать характеристики, положенные в основу определения классов защищенности СВТ.
3. Какие характеристики рассматриваются при выполнении оценки защищенности сетевых ресурсов?
4. Какой документ определяет защищенность средств вычислительной техники.
5. Сколько классов защищённости СВТ от НСД существует?

6. Верно ли утверждение «Требования ужесточаются с уменьшением номера класса»?

7. Какой вид контроля доступа реализуется для всех классов СВТ?

Практическая работа 7

Управление жизненным циклом средств аутентификации аппаратных идентификаторов с помощью средств централизованного учета и управления программно-аппаратными средствами защиты информации

Цель занятия. Рассмотреть методы управления жизненным циклом средств аутентификации аппаратных идентификаторов

Задание

1. Управление жизненным циклом средств аутентификации аппаратных идентификаторов.
2. Выполнить управление с помощью средств централизованного учета и управления программно-аппаратными средствами защиты информации

Контрольные вопросы

1. Перечислить классы защищенности АС?
2. Назвать характеристики, положенные в основу определения классов защищенности АС.
3. Как определить класс АС?
4. Перечислить необходимые признаки для группировки АС в различные классы.
5. Какие АС включаются в первую группу?
6. Для чего выполняется моделирование угроз программного приложения?
7. Какие Шаги, выполняемые при моделировании угроз?
8. Определить состав входной и выходной информации для этапа определения требований по обеспечению безопасности приложения.
9. Какие критерии используются для развертывания и инфраструктуры программного приложения?
10. Какие шаги выполняются при анализе кода программного приложения?