МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Методические указания

по выполнению лабораторных работ
по дисциплине
«УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ»
для студентов специальности 10.05.03 Информационная безопасность автоматизированных систем, специализация Анализ безопасности информационных систем

Ставрополь
2026

ВВЕДЕНИЕ

Цель и задачи освоения дисциплины

Целью освоения дисциплины «Управление информационной безопасностью» является выработка у будущего специалиста по специальности 10.05.03 Информационная безопасность автоматизированных систем специализация «Анализ безопасности информационных систем» навыков по обнаружению, оповещению об инцидентах информационной безопасности и их оценки; обучение реагировать на инциденты информационной безопасности, включая активизацию соответствующих защитных мер для предотвращения, уменьшения последствий и восстановления после негативных воздействий; анализ инцидентов информационной безопасности, введение превентивных защитных мер и улучшению общего подхода к менеджменту инцидентов информационной безопасности.

Задачи освоения дисциплины:

1. обнаруживать события информационной безопасности и эффективно их обрабатывать, также определять относятся или не относятся данные события к инцидентам информационной безопасности;
2. давать оценку инцидентам информационной безопасности;
3. минимизировать воздействие инцидентов информационной безопасности на защищенные автоматизированные системы управления.

СТРУКТУРА И СОДЕРЖАНИЕ ЛАБОРАТОРНЫХ ЗАНЯТИЙ

Лабораторная работа № 1-3 Анализ задач управления АИС и информационной безопасностью

Скажите мне честно - есть ли хоть какой-то выход из этого кошмара? - Выход всегда есть, - ответил Эркюль Пуаро.
А. Кристи «Подвиги Геркулеса»

Задание:

1. Подготовиться к публичному собеседованию по материалам лекции 1;

Вводная часть

Ввиду растущей сложности современного бизнеса компаниям приходится постоянно внедрять все новые и новые технологии, устанавливая более мощное и качественное оборудование. Для успешного использования современных информационных технологий необходимо надежное и эффективное управление не только самими сетями, но и средствами сетевой безопасности. И если в прошлом задача заключалась в управлении отдельными серверами, сетями и маршрутизаторами, то сейчас требуется обеспечить информационную безопасность корпоративных бизнес-процессов (систем). В настоящее время на первый план выходит задача создания комплексной системы управления, которая охватывает всю инфраструктуру компании и, независимо от сложности и масштаба АС, позволяет:

- централизованно и оперативно оказывать управляющие воздействия на всю информационную инфраструктуру;
- проводить регулярный аудит и всеохватывающий мониторинг, дающие объективную информацию о состоянии информационной безопасности для принятия оперативных решений;
- накапливать статистические данные о работе информационной инфраструктуры для прогнозирования ее развития.

Основная задача любой информационной системы - создание условий для работы и ведения бизнеса, облегчение и автоматизация труда людей:

1. Письменный контроль основных определений понятий дисциплины.
2. Собеседование по вопросам лекции 1: см. Л 1;
3. Отработка задания 1: см. Л 1;
4. Отработка задания 2:

5.1. Методология управления информационными системами ITIL

Согласно методологии ITIL (IT Infrastructure Library), предложенной британским Центральным компьютерным и телекоммуникационным агентством (CCTA), информационная система состоит из двух крупных блоков: информационной инфраструктуры и информационных сервисов (рис. 1).

Рис. 1. Информационная система с точки зрения методологии ITIL Информационные системы создаются для обеспечения условий функционирования информационных сервисов. Это могут быть Internet-сервисы, сервисы приложений, сервисы управления, принятия решений и т.п. Однако ни один сервис невозможно себе представить без информационной инфраструктуры.

Информационная инфраструктура является материальной основой, той средой, в которой функционируют информационные сервисы. Она представляет собой совокупность технических средств, линий связи, процедур, нормативных документов и т.п., которые обеспечивают функционирование сервисов. Качество информационных сервисов напрямую зависит от качества информационной инфраструктуры и управления ею.

Информационную инфраструктуру можно представить, как пирамиду (рис. 2), в основании которой лежат информационные ресурсы (вычислительные платформы, серверы, ПК, сети передачи данных, линии связи). Второй уровень пирамиды образуют различные приложения. Они используют ресурсы из первого слоя и обеспечивают работу сервисов таких конкретных приложений, как прикладное ПО, электронная почта, системы гарантированной доставки, базы данных, Web-сервисы и т.д. И наконец, на самом верхнем уровне функционируют приложения, обеспечивающие прохождение бизнес- и производственных процессов. Эти приложения, использующие оба нижних слоя, направлены на решение таких бизнес-задач, как управление производством, взаимодействие с заказчиками и поставщиками, финансовый учет и поддержка принятия решений.

Методология ITIL изложена в наборе всесторонних и согласованных документов, построенных на основе знаний и опыта мировых организаций, и предназначена для управления обслуживанием ИС. Библиотека ITIL состоит из более чем 40 книг, разработанных британским Центральным компьютерным и телекоммуникационным агентством (CCTA). Библиотека была создана в конце 1980-х годов, когда многие организации оказались все более зависимыми от ИС.

Рис. 2. Составляющие информационной инфраструктуры

Цель методологии ITIL - повысить эффективность ИС в выполнении бизнес- задач и уменьшить затраты на предоставление или модернизацию сервисов ИТ.

Концепция ITIL базируется на лучшей практике и опыте ведущих экспертов, консультантов, инженеров. На сегодня это наиболее целостный и полный документ, описывающий организацию управления обслуживанием ИС, своего рода стандарт де-факто.

Одним из первых способов управления сетевыми ресурсами было применение удаленного доступа к компьютеру или к иному сетевому устройству (например, к принтеру или маршрутизатору) с целью его администрирования, однако за прошедшие двадцать лет появились более сложные инструменты управления сетями. В общем случае архитектура системы управления сетью имеет вид, представленный на рис. 3. Приложение для управления сетью может выполняться на рабочем месте администратора сети или на другом компьютере. Его назначение -собирать сведения об управляемых устройствах, которые поступают от так называемых *агентов* - приложений или сервисов операционной системы, выполняющихся на управляемых устройствах.

Обычно приложение для управления сетью оперирует большими объемами подобных данных и отображает их в том или ином виде с помощью пользовательского интерфейса консоли управления, доступной администратору сети, обрабатывая происходящие в сети события. Нередко подобные приложения могут выполнять определенные операции на основе собранных ими данных, например, запускать тесты, останавливать или переконфигурировать управляемые устройства, выдавать диагностические сообщения.

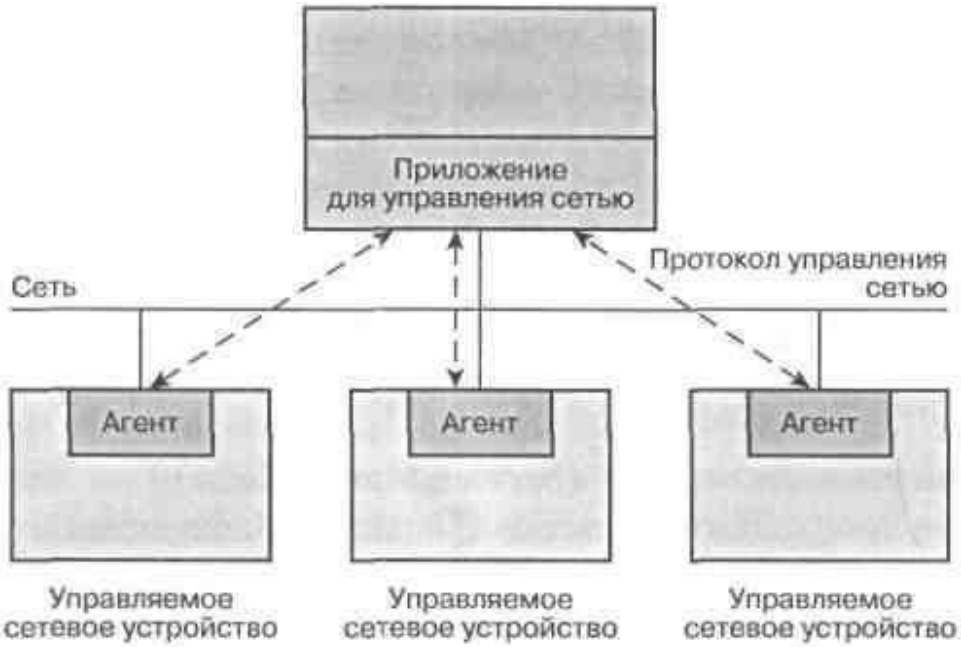


Рис. 3. Обобщенная архитектура системы управления сетью

Для взаимодействия подобных приложений с агентами обычно применяются открытые сетевые протоколы, такие как SMNP (Simple Network Management Protocol) - обычно в локальных сетях - или CMIP (Common Management Information Protocol) - обычно в случае распределенных сетей, использующих телекоммуникации, хотя некоторые производители программного обеспечения для управления сетями пользуются и собственными сетевыми протоколами.

Современные средства управления сетями могут выполнять следующие задачи:

− отслеживание сбоев в управляемых компьютерах и устройствах, определение и устранение их причин (нередко автоматическое), исправление их последствий и предотвращение сбоев (например, путем выполнения диагностических операций);

− управление конфигурированием компьютеров и сетевых устройств (в частности,инициализация, переконфигурирование и выключение управляемых сетевых устройств и компьютеров);

− управление потреблением сетевых ресурсов пользователями и группами пользователей (например, регулирование дисковых или иных квот);

− управление производительностью сетевых устройств и сервисов (с помощью сбора и анализа статистики интенсивности применения и частоты ошибок сетевых устройств и искусственной установки уровня их производительности на основе полученных данных);

− управление защитой данных с помощью контроля доступа к сетевым ресурсам на основе заранее установленной политики безопасности и уведомления администратора о попытках ее нарушения.

Методология ITIL логически группирует наиболее популярные процессы в два набора, ,представляющие основные элементы управления ИТ-сервисами:

сервисную поддержку (Service Support) и предоставление сервиса (Service Delivery).

Набор сервисной поддержки включает:

− управление конфигурацией (Configuration Management);

− взаимодействие с пользователями (Service Desk);

− управление проблемами (Problem Management);
− управление изменениями (Change Management);
− управление разработкой и распространением ПО (Software Control & Distribution).

Набор предоставляемого сервиса включает:
− управление уровнем сервиса (Service Management);
− управление производительностью (Capacity Management);
− управление доступностью (Availability Management);
− управление затратами (Cost management);
− управление непрерывностью (Contingency Management).

Многие организации используют ITIL в своей работе, поскольку эта концепция предлагает систематический и профессиональный подход к управлению информационными системами.

Первый подход заключается в интеграции средств сетевого или системного управления с механизмами управления средств защиты. Средства сетевого и системного управления ориентированы в первую очередь на управление сетью или информационными системами, то есть поддерживают традиционные действия и услуги: управление учетными записями пользователей, управление ресурсами и событиями, маршрутизацию, производительность и т.п. Ряд компаний (в их числе Cisco Systems, Computer Associates, Hewlett Packard, PLATINUM Technology, Tivoli Systems) пошли по пути интеграции механизмов управления средств защиты в традиционные системы управления сетями. Однако часто такие комплексные системы управления отличаются высокой

стоимостью, и кроме того, некоторые аспекты управления безопасностью остаются за пределами внимания этих систем.

Если использование таких комплексных решений в организации невозможно по каким-либо причинам, то имеет смысл обратить внимание на средства, предназначенные для решения только одной задачи - управления безопасностью. Например, Open Security Manager (OSM) от Check Point Software Technologies дает возможность централизованно управлять корпоративной политикой безопасности и инсталлировать ее на сетевые устройства по всей компании. Продукт OSM является одной из основных компонент технологии

OPSEC (Open Platform for Secure Enterprise Connectivity), разработанной компанией Check Point, он создает интерфейс для управления устройствами сетевой безопасности различных производителей (например, Cisco, Bay, 3Com).

Лабораторная работа № 4-6 Реализация системы управления средствами безопасности

Структурно-продуктная линия Trust Works подразделяется на агентов безопасности (Trusted Agent), центр управления (Trusted GSM Server) и консоль управления (Trusted GSM Console). Общая структурная схема решения показана на рис. 12.4. Установленный на персональном компьютере клиента, ори- ентирован на защиту индивидуального пользователя, выступающего, как прави- ло, клиентом в приложениях «клиент-сервер».

Агент безопасности, установленный на сервере приложений, ориентирован на обеспечение защиты серверных компонент распределенных приложений.

Агент безопасности, установленный на шлюзовом компьютере, обеспечивает развязку сегментов сети внутри предприятия или между предприятиями (business-to-business), решая задачи согласования политик безопасности разных сетей.

*Рис. 12.4. Общая структурная схема системы управления средствами информационной безопасности*Центр управления обеспечивает описание глобальной политики безопасности в масштабах сети, трансляцию глобальной политики в локальные политики безопасности устройств защиты, загрузку устройств защиты и контроль состояний всех агентов системы. Для организации распределенной схемы управления безопасности предприятия в системе GSM предусматривается установка нескольких (до 65535) серверов GSM.

Консоль управления предназначена для организации рабочего места администрат- ратора (администраторов) системы. Для каждого из серверов GSM может быть установлено несколько консолей, каждая из которых настраивается согласно ро- левым правам каждого администратора системы GSM.

Локальный агент безопасности представляет собой программу, размещаемую на оконечном устройстве (клиенте, сервере, шлюзе) и выполняющую следующие функции защиты:

− аутентификацию объектов политики безопасности, включая интеграцию различных сервисов аутентификации;

− определение пользователя в системе и событий, связанных с данным пользователем;

− обеспечения централизованного управления средствами безопасности и контроля доступа;

− управления ресурсами в интересах приложений, поддержку управления доступом к ресурсам прикладного уровня;

− защиту и аутентификацию трафика;

− фильтрацию трафика;

− событийное протоколирование, мониторинг, тревожную сигнализацию.
Дополнительные функции локального агента безопасности (разрабатываются в
− составе решения GSM):
− поставка криптосервиса (multiple concurrent pluggable modules);
− управление периметрами Single Sign-On (как подзадача аутентификации пользователей);− сервис в интересах защищенных приложений (криптосервис, сервис доступа к PKI, доступ к управлению безопасностью);
− сжатие трафика (IPcomp, pluggable module);
− управление резервированием сетевых ресурсов (QoS);
− функции локального агента сетевой антивирусной защиты.
Центральным элементом локального агента является процессор локальной политики безопасности (LSP processor), интерпретирующий локальную политику безопасности и распределяющий вызовы между остальными компонентами.
Защита ресурсов
Аутентификация и авторизация доступа В рамках решения реализуется ряд различных по функциональности схем аутен-тификации, каждая из которых включает тип аутентификации и способ (меха-низм) идентификации объектов.
Для выбора типа аутентификации предусмотрены следующие возможности: аутентификация пользователя при доступе к среде GSM или локальной операци онной системе, аутентификация пользователя при доступе в сеть (сегмент сети), взаимная сетевая аутентификация объектов (приложение-приложение). Для выбора способа идентификации предусмотрены следующие варианты, обычно используемые совместно в любой конфигурации: токен (смарт-карта), пароль,
«внешняя» аутентификация.
Контроль доступа при сетевых взаимодействиях При инициализации защищенного сетевого соединения от локальной операционной системы или при получении запроса на установление внешнего соединения локальные агенты безопасности на концах соединения (и/или на промежуточном шлюзе) обращаются к ЛПБ устройства и проверяют, разрешено ли установление данного соединения. В случае, если такое соединение разрешено, обеспечивается требуемый сервис защиты данного соединения, если запрещено - сетевое соединение не предоставляется.
Контроль доступа на уровне прикладных объектов
Для незащищенных распределенных приложений в GSM обеспечивается сервис разграничения прав доступа на уровне внутренних объектов данного приложения.
Контроль доступа на уровне объектов прикладного уровня обеспечивается за счет применения механизма proxy Proxy разрабатывается для каждого прикладного протокола. Предустановленным является протокол HTTP. Для построения распределенной схемы управления и снижения загрузки сети в GSM используется архитектура распределенных proxy-агентов (proxy-модуль в составе локального агента), каждый из которых:
− имеет абстрактный универсальный интерфейс, обеспечивающий модульное подключение различных proxy-фильтров; О имеет интерфейс к системе управления, но использует временный кэш для управления параметрами фильтрации; О осуществляет фильтрацию, управляемую обобщенными правилами типа:
− аутентифицировать субъект X в приложении-объекте Y;
− разрешить доступ субъекту X к объекту Y с параметрами P;
− запретить доступ субъекту X к объекту Z.
Семантика правил управления proxy-фильтром и описания субъектов и объектов доступа зависят от конкретного прикладного протокола, однако центр управления имеет

возможность регистрировать proxy-фильтры и обеспечивать управление ими в контексте общей глобальной политики безопасности.
Proxy-агент может быть установлен на шлюзе безопасности, непосредственно на сервере, исполняющем контролируемые приложения, и на клиентском месте системы.
Управление средствами защиты
Важнейшим элементом решения TrustWorks является централизованная, основанная на политике (policy based) система управления средствами сетевой и информационной безопасности масштаба предприятия. Эта система обеспечивает следующие качественные потребительские характеристики:
− высокий уровень защищенности системы управления (путем выделения защищенного периметра управления внутри сети предприятия); О расширяемость системы управления информационной безопасностью;
− высокий уровень надежности системы управления и ключевых ее компонентов;
− интеграцию с корпоративными системами общего сетевого и информационного управления;
− простую, интуитивно воспринимаемую, эргономичную и инфраструктурную среду описания, формирования, мониторинга и диагностики политики безопасности масштаба предприятия (enterprise level policy based management).
Управление осуществляется специальным программным обеспечением администратора - консолью управления. Количество и функции каждого из экземпляров установленной в системе ПО консоли управления задаются главным администратором системы в зависимости от организационной структуры предприятия. Для назначения функций каждого из рабочих мест консоли управления используется ролевой механизм разграничения прав по доступу к функциям управления (менеджмента) системы.
Функции управления GSM
В зависимости от вида управляемых объектов набор управляющих функций в GSM можно условно разбить на 3 категории:
− управление информационным каталогом;
− управление пользователями и правами доступа;
− управление правилами ГПБ.
Функции управления информационным каталогом определяют информационную составляющую GSM:
− формирование разделов каталога;
− описание услуг каталога;
− назначение и контроль сетевых ресурсов, требуемых для выполнения услуги;
− регистрация описания услуги;
− контроль состояния услуг или разделов каталога услуг;
− мониторинг исполнения услуг;
− подготовка и пересылка отчетов (протоколов) по состоянию каталога. Для управления правами доступа пользователей системы к услугам (информационным или сетевым ресурсам) GSM выполняет следующие функции:
− формирование групп пользователей по ролям и/или привилегиям доступа к услугам системы;
− формирование иерархических агрегаций пользователей по административным, территориальным или иным критериям (домены и/или департаменты);
− формирование ролей доступа пользователей к услугам (информационным или
− сетевым ресурсам);
− назначение уровней секретности для услуг и пользователей системы (поддержка мандатного механизма разграничения прав);

− назначение фиксированных прав доступа группам, ролям, агрегациям пользо- вателей или отдельным пользователям системы к информационным или сетевым ресурсам системы;
− подготовка и пересылка отчетов (протоколов) по доступу пользователей к услугам системы;
− подготовка и пересылка отчетов (протоколов) по работе администраторов системы.
Правила ГПБ ставят в соответствие конкретные свойства защиты (как для сетевых соединений, так и для доступа пользователей к информационным услугам) предустановленным уровням безопасности системы. Контроль за соблюдением правил ГПБ выполняет специальный модуль в составе сервера системы - процессор политики безопасности (Security Policy Processor), обеспечивающий следующие функции системы:
− определение каждого из уровней безопасности набором параметров защиты соединений, схемы аутентификации и разграничения прав;
− назначение уровней безопасности конкретным услугам или разделам каталога услуг;
− назначение уровней безопасности пользователям или любым агрегациям пользователей системы (группам, ролям, доменам, департаментами контроль за целостностью ГПБ (полнотой правил);
− вычисление ЛПБ локальных устройств защиты - агентов безопасности и контроль за их исполнением;
− контроль за исполнением ГПБ по различным критериям;
− подготовка и пересылка отчетов (протоколов) о состоянии системы и всех попытках нарушения ГПБ.
Каждый из администраторов системы аутентифицируется и работает с системой через консоль управления согласно предустановленным для него правам (на каталог ресурсов или его часть, на определенный ролями набор функций управления, на группы или другие наборы пользователей). Все действия любого администратора протоколируются и могут быть попарно контролируемы.
В целях обеспечения непротиворечивости с существующими у пользователя системами управления предприятия (Enterprise & Network Management System) и простоты управления в GSM реализуется тесная интеграция с наиболее популярными платформами управления (CA Unicenter TNG или HP 0V), выбор определяется менеджером продуктов.

Лабораторная работа № 7-9 Технология анализа защищенности

Цель: Усвоить последовательность анализа защищенности автоматизированной системы при построении политики информационной безопасности
Задание: Проработать материал занятия и предыдущей лекции (тема 2 Л-1) и составить блок – схему технологии анализа защищенности в рамках построения политики информационной защищенности.
В организации, использующей корпоративную информационную систему, приходится регулярно проверять, насколько реализованные или используемые механизмы защиты информации соответствуют положениям принятой в организации политики безопасности. Такая задача периодически возникает при изменении и обновлении компонентов информационной системы, изменении конфигурации операционной системы и т.п.
Однако администраторы сетей не имеют достаточно времени на проведение подобных проверок для всех узлов корпоративной сети. Поэтому специалисты отделов защиты

информации нуждаются в средствах, облегчающих анализ защищенности используемых механизмов обеспечения информационной безопасности. Этот процесс помогают автоматизировать средства анализа защищенности, называемые на Западе *сканерами безопасности* (security scanners).

Использование средств анализа защищенности позволяет определить уязвимости на узлах корпоративной сети и устранить их до того, как ими воспользуются злоумышленники. По существу, работа системы анализа защищенности аналогична действиям охранника, периодически обходящего все этажи охраняемого здания в поисках незапертых дверей, открытых окон и других

«брешей». Только в качестве здания выступает корпоративная сеть, а в качестве незакрытых окон и дверей - уязвимости. Если снова обратиться к рис. 1, поясняющему этапы развития атаки на корпоративную информационную систему, то можно заметить, что средства анализа защищенности работают на первом этапе осуществления атаки. Обнаруживая и своевременно устраняя уязвимости, они таким образом предотвращают саму возможность реализации

атаки, что позволяет снизить затраты (финансовые, ресурсные, человеческие и т.д.) на эксплуатацию средств защиты.

Технологии анализа защищенности являются действенным методом, позволяющим проанализировать и реализовать политику сетевой безопасности прежде, чем осуществится попытка ее нарушения снаружи или изнутри организации.

Средства анализа защищенности могут функционировать на сетевом уровне, уровне операционной системы и уровне приложения. Они могут проводить поиск уязвимостей, постепенно наращивая число проверок и «углубляясь» в информационную систему, исследуя все ее уровни.

Наибольшее распространение получили средства анализа защищенности сетевых сервисов и протоколов. Обусловлено это, в первую очередь, универсальностью используемых протоколов. Изученность и повсеместное использование таких протоколов, как IP, TCP, HTTP, FTP, SMTP и т.п., позволяют с высокой степенью эффективности проверять защищенность информационной системы, работающей в сетевом окружении.

Вторыми по распространенности являются средства анализа защищенности операционных систем. Обусловлено это также универсальностью и распространенностью некоторых операционных систем (например, UNIX и Windows NT). Однако из-за того, что каждый производитель вносит в операционную систему свои изменения (в качестве примера можно привести множество разновидностей ОС UNIX), средства анализа защищенности ОС анализируют в первую очередь параметры, характерные для всего семейства данной ОС. Лишь для некоторых систем предусмотрен анализ их специфичных параметров.

Средств анализа защищенности приложений на сегодняшний день не так уж много. Такие средства пока существуют только для широко распространенных прикладных систем типа Web-браузеров (Netscape Navigator, Microsoft Internet Explorer), СУБД (Microsoft SQL Server, Oracle) и т.п.

Применение средств анализа защищенности позволяет быстро определить все узлы корпоративной сети, доступные в момент проведения тестирования, выявить все используемые в сети сервисы и протоколы, их настройки и возможности несанкционированного воздействия (как изнутри корпоративной сети, так и снаружи). По результатам сканирования эти средства вырабатывают рекомендации и пошаговые меры, позволяющие устранить выявленные недостатки.

Данный метод контроля нарушений политики безопасности не может заменить специалиста по информационной безопасности. Средства анализа защищенности призваны лишь автоматизировать поиск некоторых известных уязвимостей.

Взаимодействие абонентов в любой сети базируется на использовании сетевых протоколов и сервисов, определяющих процедуру обмена информацией между двумя и более узлами. При разработке сетевых протоколов и сервисов к ним предъявлялись требования (обычно явно недостаточные) по обеспечению безопасности обрабатываемой информации.

Поэтому постоянно появляются сообщения об обнаруженных в сетевых протоколах уязвимостях. В результате возникает потребность в постоянной проверке всех используемых в корпоративной сети протоколов и сервисов.

Системы анализа защищенности выполняют серию тестов по обнаружению уязвимостей. Эти тесты аналогичны применяемым злоумышленниками при осуществлении атак на корпоративные сети.

Сканирование с целью обнаружения уязвимостей начинается с получения предварительной информации о проверяемой системе, в частности о разрешенных протоколах и открытых портах, используемой версии операционной системы и т.п. Заканчивается сканирование попытками имитации проникновения; используются широко известные атаки, например подбор пароля методом полного перебора (brute force - «грубая сила»).

При помощи средств анализа защищенности на уровне сети можно тестировать не только возможность несанкционированного доступа в корпоративную сеть из Internet. Эти же средства могут быть использованы для аналогичной проверки во внутренней сети организации. Системы анализа защищенности на уровне сети могут быть использованы как для оценки уровня безопасности организации, так и для контроля эффективности настройки сетевого программного и аппаратного обеспечения.

В настоящее время известно более десятка различных средств, автоматизирующих поиск уязвимостей сетевых протоколов и сервисов. Одно из первых таких средств - свободно распространяемая система анализа защищенности UNIX-систем SATAN (Security Administrator Tool for Analyzing Networks), разработанная В. Венема и Д. Фармером. Среди коммерческих систем анализа защищенности можно назвать Internet Scanner компании Internet Security Systems Inc., NetSonar компании Cisco, CyberCop Scanner компании Network Associates и ряд других.

Средства анализа защищенности данного класса анализируют уязвимость не только сетевых сервисов и протоколов, но и системного и прикладного программного обеспечения, отвечающего за работус сетью. К такому обеспечению можно отнести Web-, FTP- и почтовые серверы, межсетевые экраны, браузеры и т.п.

Некоторые из предлагаемых на рынке систем проводят не только анализ защищенности программного обеспечения, но и сканирование аппаратных средств. К таким аппаратным средствам относится коммутирующее и маршрутизирующее оборудование.

Средства этого класса предназначены для проверки настроек операционной системы, влияющих на ее защищенность. К таким настройкам можно отнести:

− учетные записи пользователей (accounts), например, длину пароля и срок его действия;

− права пользователей на доступ к критичным системным файлам; О уязвимые системные файлы; О установленные патчи (patches) и т.п.

Системы анализа защищенности на уровне ОС также могут быть использованы для контроля конфигурации операционных систем.

В отличие от средств анализа защищенности сетевого уровня, эти системы проводят сканирование не снаружи, а изнутри анализируемой ОС, то есть не имитируют атаки внешних злоумышленников. Кроме обнаружения уязвимостей некоторые системы анализа защищенности на уровне ОС (например, System Scanner компании Internet Security Systems)

автоматически устраняют ряд обнаруженных проблем или корректируют параметры системы, не удовлетворяющие политике безопасности, принятой в организации.
Как уже отмечалось, средств анализа защищенности операционной системы существует меньше, чем средств проверки сети. Среди первых
известных систем можно назвать COPS (Computerized Oracle and Password System), разработанную одним из авторов системы SATAN Д. Фармером совместно с Ю. Спаффордом из лаборатории COAST. Также широко известны системы System Security Scanner и Security Policy Manager компании Internet Security Systems Inc., Kane Security Analyst компании Intrusion Detection и др.
Остановимся на некоторых общих характеристиках и требованиях к средствам анализа защищенности, которые нужно учитывать при их выборе и приобретении.
Обязательное условие, которое предъявляется к выбираемой системе, - отсутствие необходимости изменения сетевой инфраструктуры предприятия. В противном случае затраты на такую реорганизацию могут превысить стоимость самой системы анализа защищенности. В настоящий момент только разработка Internet Scanner компании Internet Security Systems удовлетворяет данному требованию.

При неправильном применении средств анализа защищенности ими могут воспользоваться злоумышленники для проникновения в корпоративную сеть. Поэтому средства анализа защищенности должны быть обеспечены механизмами разграничения доступа к своим компонентам и собранным данным. Форма представления данных в отчетах имеет немаловажное значение. Документ, насыщенный только текстовой информацией, не принесет пользы.
Использование же графики наглядно продемонстрирует руководству все проблемы с безопасностью в сети организации. Обязательное условие при выборе средств анализа защищенности - наличие в отчетах рекомендаций по устранению найденных проблем.
Постоянное обнаружение новых уязвимостей требует, чтобы система анализа защищенности предусматривала возможность пополнения базы данных уязвимостей.
Это может быть реализовано как при помощи специального языка описания уязвимостей (например, APX в системах компании ISS, CASL в системе CyberCop Scanner), так и путем периодического пополнения уязвимостей, обеспечиваемого производителем системы. Для последующего анализа изменений уровня защищенности узлов корпоративной сети выбираемое средство должно позволять накапливать сведения о проведенных сеансах сканирования.
Эффективность применения систем анализа защищенности будет достигнута только в том случае, если их производитель постоянно обеспечивает свои продукты соответствующей поддержкой, учитывающей последние изменения в области обеспечения информационной безопасности. Информация об уязвимостях должна постоянно пополняться. Например, система SATAN не может быть рекомендована как надежное и эффективное средство, так как последние изменения в нее вносились несколько лет назад.
Однако следует отметить, что информация об уязвимости обычно появляется в базе данных системы не раньше, чем найдется ей «противоядие». Это является определенным недостатком всех способов поиска уязвимостей, поскольку злоумышленники могут воспользоваться имеющейся информацией до того, как появится способ устранения найденной уязвимости.
Лабораторная работа№ 4
Постановка задач синтеза систем в конфликтных условиях как минимаксная задача

При постановке задачи синтеза системы (процесса, алгоритма, стратегии,...) полагаются заданными [1-12]: множество X рассматриваемых в задаче объектов (допустимых вариантов построения систем), множество Y условий функционирования систем и функционал $Q : X \times Y \to R$ (где R - множество вещественных чисел),

определяющий значение $Q\{X,Y\}$ обобщенного показателя эффективности (ОПЭ) для любых элементов $X \in X$ и $Y \in Y$. Процедура задания конструкций X , Y и $Q\{\}\cdot$ и их интерпретация в терминах вариантов построения и характеристик реальных объектов составляют неформальную сторону модели класса исследуемых систем. Формальная часть модели заключается в дальнейшем использовании данных конструкций для постановки и решения математических задач синтеза систем.

$Q\{\}\cdot$

Важным свойством класса условий Y , приводящим к специфическим задачам синтеза систем, является их конфликтность. Сущность конфликтной среды заключается в том, что конкретизация элемента $Y \in Y$ для данной системы X может осуществляться противной стороной (противником), целью которой является решение противоположной задачи (т.е. уменьшение значения ОПЭ).

Целесообразность рассмотрения задачи синтеза в данном случае обусловлена практической необходимостью проектирования систем, функционирование которых предполагается при применении противником средств, специально разработанных для подавления проектируемой системы.

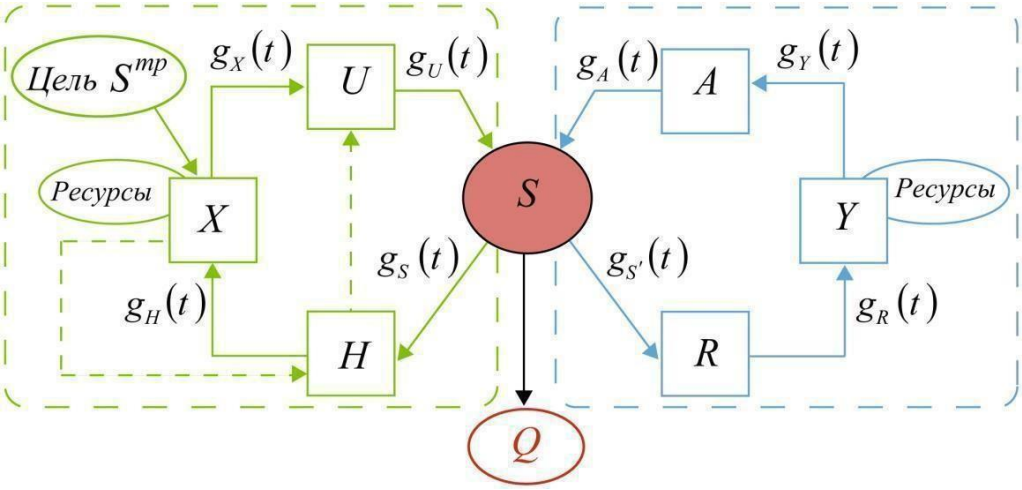
Пусть, например, для функционирования в конфликтных условиях, определенных классом Y , разработана и внедрена система $X \in X$. Это решение задачи оптимизации противодействия

Лабораторная работа № 10-12 Элементы обобщенной модели взаимодействия ПДС

Для содержательной постановки и решения задач синтеза систем связи в условиях оптимизированного противодействия необходимы конкретизация структуры конструкций X , Y , Q{}· и их интерпретация в терминах вариантов построения и характеристик реальных объектов. С этой целью процесс функционирования системы при воздействии на нее подсистемы управления, противодействующей системы, а также совокупности случайных факторов и описывается обобщенной динамической моделью взаимодействия систем, представленной функциональной схемой на рис.1.

Обобщенная модель взаимодействия конфликтующих систем (макрообъекта *W*)

Компоненты обобщенной модели макрообъекта W



H - канал наблюдения, *R - канал разведки,*

U - канал управления, *Y - СПР на подавление,*

X - СПР на управление, *A - канал подавления,*

Q – обобщенный показатель эффективности ЗАС.

В соответствии с данной моделью макрообъект, описывающий совокупность взаимодействующих элементов СВС и СП, представляется в виде композиции элементов: *S* - управляемого объекта (УО), *X* - системы (подсистемы) принятия решений на управление (СПРУ), ^{H} - канала наблюдения (КН), ^{U} - канала управления

Задача построения управляемой системы рассматривается как задача синтеза стратегии (оператора) управления ее состоянием. При этом к СПРУ и СПРП относятся все неизвестные (искомые) в задаче синтеза системы элементы, а остальные объекты модели (УО, КН, КУ, КР, КП) задают имеющиеся ограничения на реализуемые процессы управления и подавления, а также воздействия этих процессов на состояние УО.

УО представляет собой совокупность всех тех элементов системы:

- на управление (синтез стратегии управления) которыми направляется задача;
- наблюдение за которыми целесообразно учитывать при выработке решения на управление состояниями системы;
- наблюдение за которыми может оказаться полезным СПРП для выработки решения на подавление системы.

СПРУ представляет собой совокупность всех органов, выполняющих функции принятия решений на управление УО или его отдельными элементами.

КН является подсистемой, обеспечивающей сбор сведений СПРУ о состоянии УО,

Кроме того, отдельные из введенных объектов могут представляться в виде композиции составляющих элементов, что позволяет более просто задавать и интерпретировать их описания. В этом отношении существенной является декомпозиция СПРУ по подсистемам принятия решений различных уровней иерархии, которая в задачах синтеза обеспечивает задание дополнительных ограничений на класс допустимых стратегий принятия решений для предварительно определенных структур СПРУ.

В ряде случаев могут оказаться целесообразными декомпозиция КУ с выделением из него элементов, определяющих зависимость реализуемого управления от состояния УО (пунктирная линия на рис.1), а также выделение из КП элементов, характеризующих ресурс

противодействующей системы и определяющих, таким образом, ограничения на реализуемые воздействия СПРП. Вместе с тем следует отметить, что с позиций решения задачи соответствующие
модификации являются непринципиальными, поскольку все заданные особенности построения СПРУ, КН, КУ, СПРП, КР и КП могут быть учтены в ограничениях на классы допустимых решений СПРУ и СПРП [2,3, 5,6] . По сути дела все задачи, формулируемые на представленной модели, допускают адекватную постановку при исключении из рассмотрения КН, КР, КУ и КП: выделение данных элементов, является удобным лишь с точки зрения интерпретации конструкций X и Y .

СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

1. А.А. Торокин. Инженерно- Техническая защита информации», Учебное пособие Москва Гелиос 2009 г.
2. Г.А. Бузов, С.В. Калинин, А.В. Кондратьев, Учебное пособие «Защита от утечки информации по техническим каналам», Москва Телеком 2010 г.
3. Учебное пособие «Комплексный технический контроль эффективности мер безопасности систем управления в органах внутренних дел», Москва Телеком 2006 г.
4. Ярочкин В.И. Информационная безопасность: Учебник.-М.: Академпроект, 2010-640с.