Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.056

Сахаров
Павел Андреевич

Модель и средства информационной безопасности в корпоративной системе управления

АВТОРЕФЕРАТ
на соискание степени магистра техники и технологии
по специальности 1-45 81 01 «Инфокоммуникационные системы и сети»

_____

Научный руководитель
Вишняков Владимир Анатольевич
д. техн. наук, профессор,
профессор кафедры ЗИ БГУИР

_____

Минск 2017

ВВЕДЕНИЕ

Защита данных в компьютерных сетях становится одной из самых открытых проблем в современных информационно-вычислительных системах. На сегодняшний день сформулировано три базовых принципа информационной безопасности, задачей которой является обеспечение:

- целостности данных - защита от сбоев, ведущих к потере информации или ее уничтожения;
- конфиденциальности информации;
- доступности информации для авторизованных пользователей.

Рассматривая проблемы, связанные с защитой данных в сети, возникает вопрос о классификации сбоев и несанкционированности доступа, что ведет к потере или нежелательному изменению данных. Это могут быть сбои оборудования (кабельной системы, дисковых систем, серверов, рабочих станций и т.д.), потери информации (из-за инфицирования компьютерными вирусами, неправильного хранения архивных данных, нарушений прав доступа к данным), некорректная работа пользователей и обслуживающего персонала. Перечисленные нарушения работы в сети вызвали необходимость создания различных видов защиты информации. Условно их можно разделить на три класса:

- средства физической защиты;
- программные средства (антивирусные программы, системы разграничения полномочий, программные средства контроля доступа);
- административные меры защиты (доступ в помещения, разработка стратегий безопасности фирмы и т.д.

Объектом являются информационные системы.

Предметом являются модели информационной безопасности информационных систем.

Целью является изучение моделей информационной безопасности информационных систем и прикладных областей их применения.

Задачи:

- изучить принципы обеспечения информационной безопасности;
- проанализировать формальные модели информационной безопасности;
- выявить недостатки существующих стандартов по обеспечению информационной безопасности;
- изучить наиболее распространенные угрозы информационной безопасности;
- изучить информационную безопасность сети и информационную безопасность общества в шифровании данных.

КРАТКАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Работа выполнялась по теме «Модель и средства информационной безопасности в корпоративной системе управления».

Проведённая работа по диссертационной тематике соответствует мировым тенденциям в сфере телекоммуникаций. Рассмотренные технологии обеспечения информационной безопасности отражают современные тенденции в области проектирования и построения моделей и средств информационной безопасности на предприятиях.

Целью данной работы является выбор оптимальных решений для обеспечения таких важных вопросов в корпоративной системе, как безопасность, доступность и защищенность предоставляемой информации.

Для достижения цели необходимо решить следующие задачи:

– изучить принципы обеспечения информационной безопасности;

– проанализировать формальные модели информационной безопасности;

– выявить недостатки существующих стандартов по обеспечению информационной безопасности;

– изучить наиболее распространенные угрозы информационной безопасности;

– изучить информационную безопасность сети и информационную безопасность общества в шифровании данных.

Общая тенденция развития интеллектуальных и информационных технологий показывает, что модели и средства обработки информации на ее основе получает все большее развитие и распространение в управлении и информационной безопасности. Этому способствует развитие сетевого корпоративного управления, интеллектуализации бизнеса, исследованиям в области обработки знаний с использованием семантического Веб-пространства.

Особый интерес представляют модели, архитектуры и средства защиты информации в корпоративных информационных системах (КИС), которые и обуславливают актуальность исследований в данной магистерской работе.

Для поддержания режима информационной безопасности особенно важны программно-технические меры, поскольку основная угроза компьютерным системам исходит от них самих: сбои оборудования, ошибки программного обеспечения, промахи пользователей и администраторов и т. п. Напомним названия ключевых механизмов обеспечения информационной безопасности:

- идентификация и аутентификация;
- управление доступом;
- протоколирование и аудит;
- криптография;
- экранирование.

Эффективным средством противодействия различным угрозам информационной безопасности является закрытие информации методами криптографического преобразования.

Модель проблемной ситуации в области информационной безопасности (ИБ) содержит набор из трех взаимодействующих систем: проблемы довольной, решения проблем и управляющего директора, который разработан для того, чтобы проблема исчезла или ослабла. Ближайшие или существенная среда, с которой контактирует DIS это понимается как взаимодействие совокупности потенциально возможных угроз информационной безопасности. Требование постоянно нарастающим спецификации приводит к созданию модели структуры системы, проблема модели объекта защиты и модели угроз.

Модель три уровня защиты в системе управления информационной безопасностью является комплекс программно-аппаратных средств, которые в том числе: первая граница (периметр объекта защиты) - набор функциональных подсистем защиты от внешних вторжений злоумышленником; вторая граница набора средств защиты сетевого сегмента от удаленных и локальных сетевых вторжений; третья граница включает в себя набор средств защиты отдельного компьютера или сервера.

Первым направлением в СЗИ является дальнейшая разработка моделей, методов, архитектур и аппаратно-программных средств управления ЗИ для решения проблемы защиты КИС и облачной инструментальной платформы проектирования интеллектуальных систем на основе семантических технологий. Другим направлением СЗИ является разработка моделей, методов, архитектур и аппаратно-программных средств сбора, структуризации информации из Интернете, формирования специализированных баз знаний и поддержки принятия решений (на базе ИТ) по всему накопленному аспекту задач ИБ.

Предложена структура многоагентной СОА, включающая в себя множество взаимодействующих интеллектуальных агентов и соответствующая выделенным в ходе анализа типовым компонентам информационной системы и источникам сведений, подлежащих анализу для задачи обнаружения атак.

Обобщённая структура системы управления защитой информации в корпоративной информационной системы включает 2 контура. В контуре организационно-технического управления создаются механизмы управления ЗИ при изменении инфраструктуры, бизнес-приложений, планов обработки информации и соответствующих им требований к уровню защищенности информации. Контур включает: систему интеллектуальной поддержки принятия решений по выбору стратегии защиты, систему оценки уровня защищенности (риска), управляющее воздействие реализуется сотрудниками отдела информационной безопасности. В контуре оперативного управления формируется оперативная командная информация, которая доводится до объекта управления администратором безопасности или автоматически с

помощью средств реализации управляющих воздействий на встроенные в средства защиты управляющие модули.

Предложена архитектура многоагентной СОА, включающая в себя множество взаимодействующих интеллектуальных агентов и оответствующая выделенным в ходе анализа типовым компонентам информационной системы и источникам сведений, подлежащих анализу для задачи обнаружения атак [8]. Обобщенная архитектура системы управления защитой информации в корпоративной информационной системы включает 2 контура В контуре организационно-технического управления создаются механизмы управления ЗИ при изменении инфраструктуры, бизнес-приложений, планов обработки информации и соответствующих им требований к уровню защищенности информации. В контуре оперативного управления формируется оперативная командная информация, которая доводится до объекта управления администратором безопасности или автоматически с помощью средств реализации управляющих воздействий на встроенные в средства защиты управляющие модули.

КРАТКОЕ СОДЕРЖАНИЕ

Создание всеобщего информационного пространства и практически повсеместное применение персональных компьютеров, и внедрение компьютерных систем породило необходимость решения комплексной проблемы защиты информации.

В первой главе: самой распространённой на практике является дискреционная модель. В её основе лежат следующие положения:

- все субъекты и объекты должны быть идентифицированы;
- права доступа субъекта к объекту системы определяются на основании некоторого внешнего правила.

Отношения «субъекты-объекты» можно представить в виде матрицы доступа, в строках которой перечислены субъекты, в столбцах объекты ИС, а в клетках, на пересечении строк и столбцов, записаны дополнительные условия и разрешенные виды доступа. Таким образом, реализация управления доступом заключается в проверке строк матрицы, соответствующей объекту и анализируются права доступа к этому объекту для текущего субъекта.

Достоинство модели – относительно простая реализация соответствующих механизмов защиты. Недостатки – статичность модели и излишне детализированный уровень описания отношений субъектов и объектов, как следствие, усложнение администрирование и возникновение ошибок.

Основная цель мандатной политики – предотвращение утечки информации от объектов с высоким доступом к объектам низким уровнем доступа. Важное достоинство мандатной модели – формальное доказательство утверждения: если начальное состояние системы безопасно, и все переходы системы из состояния в состояние не нарушает ограничений, сформулированных политикой безопасности, то любое состояние системы безопасно.

Недостаток мандатной модели – сложность реализации. Множество операций ограничивается операциями чтения (поток данных направлен от объекта к субъекту) и записи (поток направлен от субъекта к объекту).

Под угрозой информационной безопасности КС обычно понимают потенциально возможное событие, действие, процесс или явление, которое может оказать нежелательное воздействие на систему и информацию, которая в ней хранится и обрабатывается

Противодействие многочисленным угрозам информационной безопасности предусматривает комплексное использование различных способов и мероприятий организационного, правового, инженерно-технического, программно-аппаратного, криптографического характера и т.п.

Организационные мероприятия по защите включают в себя совокупность действий по подбору и проверке персонала, участвующего в подготовке и эксплуатации программ и информации, строгое регламентирование процесса разработки и функционирования КС.

К правовым мерам и средствам защиты относятся действующие в стране законы, нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушение.

Во второй главе: инженерно-технические средства защиты достаточно многообразны и включают в себя физико-технические, аппаратные, технологические, программные, криптографические и другие средства. Данные средства обеспечивают следующие рубежи защиты: контролируемая территория, здание, помещение, отдельные устройства вместе с носителями информации.

Программно-аппаратные средства защиты непосредственно применяются в компьютерах и компьютерных сетях, содержат различные встраиваемые в КС электронные, электромеханические устройства. Специальные пакеты программ или отдельные программы реализуют такие функции защиты, как разграничение и контроль доступа к ресурсам, регистрация и анализ протекающих процессов, событий, пользователей, предотвращение возможных разрушительных воздействий на ресурсы и другие.

Эффективным средством противодействия различным угрозам информационной безопасности является закрытие информации методами криптографического (от греч. Kryptos - тайный) преобразования. В результате такого преобразования защищаемая информация становится недоступной для ознакомления и непосредственного использования лицами, не имеющими на это полномочий.

Первым направлением в СЗИ является дальнейшая разработка моделей, методов, архитектур и аппаратно-программных средств управления ЗИ для решения проблемы защиты КИС и облачной инструментальной платформы проектирования интеллектуальных систем на основе семантических технологий. Другим направлением СЗИ является разработка моделей, методов, архитектур и аппаратно-программных средств сбора, структуризации информации из Интернете, формирования специализированных баз знаний и поддержки принятия решений (на базе ИТ) по всему накопленному аспекту задач ИБ.

В третьей главе предложена структура многоагентной СОА, включающая в себя множество взаимодействующих интеллектуальных агентов и соответствующая выделенным в ходе анализа типовым компонентам информационной системы и источникам сведений, подлежащих анализу для задачи обнаружения атак.

Обобщённая структура системы управления защитой информации в корпоративной информационной системы включает 2 контура. В контуре организационно-технического управления создаются механизмы управления ЗИ при изменении инфраструктуры, бизнес-приложений, планов обработки информации и соответствующих им требований к уровню защищенности информации. Контур включает: систему интеллектуальной поддержки принятия решений по выбору стратегии защиты, систему оценки уровня защищенности (риска), управляющее воздействие реализуется сотрудниками

отдела информационной безопасности. В контуре оперативного управления формируется оперативная командная информация, которая доводится до объекта управления администратором безопасности или автоматически с помощью средств реализации управляющих воздействий на встроенные в средства защиты управляющие модули.

ЗАКЛЮЧЕНИЕ

Информационная безопасность АИС должна обеспечиваться комплексно на всех этапах технологической обработки данных и во всех режимах функционирования, в том числе при проведении ремонтных и регламентных работ

И этот комплекс мероприятий по обеспечению информационной безопасности должен быть непрерывен во времени и пространстве. Но не стоит забывать о простоте применения защитных мер и средств. При проектировании систем защиты информации необходимо помнить, что реализация предлагаемых мер и средств будет проводится пользователями (часто не являющихся специалистами в области ИБ). Поэтому для повышения эффективности мер защиты необходимо, чтобы алгоритм работы с ними был понятен пользователю. Кроме того, используемые средства и механизмы информационной безопасности не должны нарушать нормальную работу пользователя с автоматизированной системой

Самой распространённой на практике является дискреционная модель. Достоинство модели –относительно простая реализация соответствующих механизмов защиты. Недостатки – статичность модели и излишне детализированный уровень описания отношений субъектов и объектов, как следствие, усложнение администрирование и возникновение ошибок.

С целью устранения недостатков матричных моделей были разработаны многоуровневые модели. Многоуровневые модели защиты находятся гораздо ближе к потребностям реальной жизни, чем матричные, представляют собой лучшую основу для построения автоматизированных систем разграничения доступа. Основная цель мандатной политики – предотвращение утечки информации от объектов с высоким доступом к объектам низким уровнем доступа

Нарушение политики обеспечения информационной безопасности может подвергнуть локальную сеть и циркулирующую в ней информацию недопустимому риску. Поскольку наиболее уязвимым звеном любой информационной системы является человек, особое значение приобретает воспитание законопослушности сотрудников по отношению к законам и правилам информационной безопасности. Случаи нарушения этих законов и правил со стороны персонала должны рассматриваться руководством для принятия мер вплоть до увольнения

Из рассмотренного становится очевидно, что обеспечение информационной безопасности является комплексной задачей. Это обусловлено тем, что информационная среда является сложным многоплановым механизмом, в котором действуют такие компоненты, как электронное оборудование, программное обеспечение, персонал.

Для решения проблемы обеспечения информационной безопасности необходимо применение законодательных, организационных и программно-технических мер. Пренебрежение хотя бы одним из аспектов этой проблемы может привести к утрате или утечке информации, стоимость и роль которой в жизни современного общества приобретает все более важное значение.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1) Сахаров П. А. Структура многоагентной системы обнаружения атак / П. А. Сахаров // Эволюция, прогресс и модернизация: материалы Международная научно-практическая конференция аспирантов, студентов и магистрантов, 31 января 2017 г./ НОО Профессиональная наука www.scipro.ru. – Санкт-Петербург, 2017 – в печати.