



Введение

Глава 1. Необходимость и задачи защиты информации в автоматизированных системах

1.1. Актуальность проблемы защиты информации

- Роль человеческого фактора в обеспечении защиты информации
- 1.1.1. в автоматизированных системах
- 1.1.2. Понятие информационной войны
- 1.1.3. Основные понятия и термины
- 1.1.4. Особенности современных автоматизированных систем
- 1.1.5. Особенности информационных отношений между субъектами
- Классификация методов и средств защиты информации от несанкционированного доступа
- 1.1.6.
- 1.1.7. Механизмы защиты информации от несанкционированного доступа

Требования к системам и средствам защиты

1.2. информации от несанкционированного доступа

- 1.2.1. Государственные требования к построению систем защиты информации
- Особые требования к криптографическим средствам систем защиты информации
- 1.2.2. от несанкционированного доступа
- 1.2.3. Классификация автоматизированных систем и требования по защите информации
- Показатели защищенности средств вычислительной техники по защите
- 1.2.4. информации от несанкционированного доступа
- Соответствие классов защищенности АС различным уровням
- 1.2.5. конфиденциальности
- 1.2.6. Классификация информационных систем персональных данных
- Новое поколение нормативно-технических документов по безопасности
- 1.2.7. информации

1.3. Разработка модели разграничения доступа к информации

- 1.3.1. Политика безопасности
- 1.3.2. Состав и содержание документов политики безопасности
- 1.3.3. Определение перечня защищаемых ресурсов и их критичности
- Определение категорий персонала и программно-аппаратных средств, на которые
- 1.3.4. распространяется политика безопасности
- 1.3.5. Определение угроз безопасности информации
- 1.3.6. Принципы построения систем защиты информации
- Формирование требований к построению систем защиты информации и порядок
- 1.3.7. подбора соответствующих программно-аппаратных средств
- Определение уязвимостей автоматизированной системы и выбор средств защиты
- 1.3.8. информации

Глава 2. Средства защиты информации

- 2.1. Системная классификация средств защиты информации
- 2.2. Аппаратные средства защиты информации
- Основные принципы функционирования аппаратных средств защиты
- 2.3. информации
- 2.4. Программные средства защиты информации
- 2.5. Основные принципы функционирования программных средств защиты
- 2.6. Угрозы перевода программной системы защиты в пассивное состояние

Глава 3. Управление доступом в компьютерных системах

- 3.1. Разграничение доступа к информации
- 3.1.1. Идентификация и аутентификация субъектов и объектов компьютерных систем

- 3.1.2. Классификация задач по назначению защищаемого объекта
- 3.1.3. Идентифицирующая информация. Протоколы аутентификации
- 3.1.4. Подходы к реализации средств идентификации и аутентификации. Средства аутентификации пользователей
- 3.2. Основные подходы к защите данных от несанкционированного доступа
 - 3.2.1. Управление информационными потоками. Достоверная вычислительная база
 - 3.2.2. Иерархический доступ к файлу
 - 3.2.3. Доступ к данным со стороны процесса. Понятие скрытого доступа
- 3.3. Модели управления доступом
 - 3.3.1. Абстрактные модели доступа
 - 3.3.2. Многоуровневые (мандатные) модели
 - 3.3.3. Выбор модели
 - 3.3.4. Корректность и полнота реализации разграничительной политики доступа
- 3.4. Защита информации средствами операционных систем
 - 3.4.1. Защита информации в операционной системе UNIX
 - 3.4.2. Особенности защиты информации в сетевой операционной системе Windows
 - 3.4.3. Сравнительный анализ реализации встроенных моделей защиты информации в операционных системах
 - 3.4.4. Недостатки защитных механизмов ОС семейства Unix и Windows

Глава 4. Задачи контроля в обеспечении безопасности информации

- Методы контроля доступа к ресурсам компьютерной системы. Способы фиксации факта доступа к файлам
- 4.1. Структура и функции подсистемы контроля доступа программ и пользователей
- 4.2. Средства ведения и анализа системных журналов
- 4.3. Средства контроля за процессами. Свойства процессов и управление ими
- 4.4. Средства поиска остаточной информации на машинных носителях
- 4.5. информации
- 4.6. Средства гарантированного удаления информации

Глава 5. Разрушающие программные воздействия и защита от них

- 5.1. Сущность разрушающих программных воздействий
 - Модели взаимодействия прикладных программ и программы-злоумышленника
- 5.2. Классификация разрушающих программных средств и их воздействий
- 5.3. Методы внедрения разрушающих программных средств
 - Компьютерные вирусы как особый класс разрушающего программного воздействия
- 5.4. Классификация компьютерных вирусов
 - 5.5.1. Особенности распространения и жизненный цикл вирусов
- 5.5. Принципы и методы защиты от разрушающих программных воздействий
 - Требования ФСТЭК России к программному обеспечению СЗИ и его классификация по уровню контроля отсутствия недеklarированных возможностей
 - 5.6.1. Необходимые и достаточные условия недопущения разрушающего воздействия
 - 5.6.2. Организационные средства защиты от компьютерных вирусов
 - 5.6.3.
- 5.7. Построение и принципы работы типовых антивирусных средств

Глава 6. Обеспечение целостности информации

- 6.1. Проблема обеспечения целостности информации
- 6.2. Способы и средства обеспечения целостности информации

- 6.3. Защита файлов от изменений
- 6.4. Криптографические средства обеспечения целостности информации
 - 6.4.1. Способы выявления изменений
 - 6.4.2. Криптографические хэш-функции
- 6.5. Электронная подпись
 - 6.5.1. Прямая и арбитражная электронные подписи
 - 6.5.2. Угрозы электронной подписи
 - 6.5.3. Системы электронной подписи

Глава 7. Программно-аппаратные средства шифрования

Основные принципы криптографической защиты информации

- 7.1. в автоматизированных системах
 - Задачи, решаемые криптографическими средствами в автоматизированных системах
 - 7.1.1. Стойкость криптографических алгоритмов
 - 7.1.2. Алгоритмы криптографических преобразований и их характеристики
 - 7.1.3. Симметричные криптоалгоритмы
 - 7.1.4. Асимметричные (с открытым ключом) криптоалгоритмы
 - 7.1.5. Уязвимости и защита алгоритма шифрования
 - 7.1.6. Невозможность применения стойких криптоалгоритмов
 - 7.1.7. Неправильная реализация криптоалгоритмов
 - 7.1.8. Неправильное применение криптоалгоритмов
 - 7.1.9. Человеческий фактор
- 7.2. Программно-аппаратные средства шифрования
 - 7.2.1. Принцип чувствительной области и принцип главного ключа
 - 7.2.2. Необходимые и достаточные функции аппаратного средства криптозащиты
 - 7.2.3. Аппаратная реализация
 - 7.2.4. Программная реализация
 - 7.2.5. Программно-аппаратная реализация
 - 7.2.6. Построение аппаратных компонентов криптозащиты данных

Глава 8. Методы распределения и хранения ключевой и парольной информации

- 8.1. Построение ключевых систем
 - 8.1.1. Генерация ключей
 - 8.1.2. Проблемы распределения ключей в автоматизированных системах
 - 8.1.3. Пароли и ключи
- 8.2. Организация распределения ключевой и парольной информации
 - 8.2.1. Прямой обмен ключами
 - 8.2.2. Обмен ключами через посредника
 - 8.2.3. Централизованное распределение ключевой информации
- 8.3. Методы распределения ключей и паролей в распределенных системах
 - 8.3.1. Цифровые сертификаты
 - 8.3.2. Механизмы контроля использования ключей
 - 8.3.3. Организация хранения ключей и паролей
 - 8.3.4. Хранение ключей и паролей на дисках

Литература



На современном этапе развития нашего общества многие традиционные ресурсы человеческого прогресса постепенно утрачивают свое первостепенное значение. На смену им приходит новый ресурс, единственный не убывающий, а растущий со временем -- информационный.

Информационные технологии (ИТ) все глубже проникают во многие сферы жизни общества. Информация стала товаром, который можно приобрести, продать, обменять. При этом стоимость информации часто в сотни раз превосходит стоимость компьютерной системы (КС), в которой она хранится и обрабатывается. Этот процесс становится настолько масштабным, что затрагивает жизненные интересы государства, в том числе и в области информационной безопасности.

Современная информационная система (ИС) представляет собой сложную систему, состоящую из большого числа компонентов различной степени автономности, которые связаны между собой и обмениваются данными. Автоматизированные системы управления (АСУ) широко применяются в атомной, нефтегазоперерабатывающей, химической промышленности, на транспорте, в навигационных системах, системах управления государством и других областях. Практически каждый компонент автоматизированной системы (АС) может подвергнуться внешнему воздействию или выйти из строя.

Таким образом, в настоящее время от степени защищенности информационных технологий зависит благополучие, а порой и жизнь многих людей. Вывод из строя автоматизированных систем может повлечь сбой технологического цикла предприятия, систем управления и сопровождения транспорта и, как следствие, привести к авариям и катастрофам с гибелью населения. Нарушение в информационных процессах может повлечь за собой экономический, экологический или военный кризис. Такова плата за усложнение и повсеместное распространение автоматизированных систем обработки информации.

Наряду с этим важное значение приобретает защита национальных информационных ресурсов, обусловленная расширением доступа к ним через открытые информационные сети типа Интернет. Экспоненциально увеличивается число компьютерных преступлений.

Несмотря на то что современные операционные системы (ОС), такие как Windows, Linux или MSVC, имеют собственные подсистемы защиты, актуальность создания дополнительных средств защиты сохраняется. Дело в том, что большинство систем не способны защитить данные, находящиеся за их пределами. К наиболее уязвимым местам, через которые обычно пытаются проникнуть злоумышленники, относятся открытые системы, системы, поддерживающие технологию подключения периферийных устройств в режиме plug-and-play, средства централизованной удаленной поддержки, коммутируемые каналы удаленного доступа и недостаточно надежные технологии шифрования.

В результате возникает проблема защиты информации в автоматизированных системах, которая является одной из основных составляющих обеспечения безопасности информации.

Особая актуальность задачи обеспечения информационной безопасности (ИБ) компьютерных систем в Российской Федерации на современном этапе отражена в таких основополагающих государственных документах, как Федеральный закон РФ "О безопасности", "Стратегия национальной безопасности РФ до 2020 года" и "Доктрина

информационной безопасности РФ". В них отмечается, что именно информационная инфраструктура общества -- первая мишень информационного терроризма.

Не стоит думать, что ввиду унаследованной информационной замкнутости, определенной технологической отсталости Россия менее уязвима, чем другие государства, -- скорее наоборот. Как раз высокая степень централизации структур государственного управления российской экономикой может привести к губительным последствиям в результате информационной агрессии или террористических действий.

Конечно, российские спецслужбы располагают необходимыми средствами и известным опытом предотвращения перехвата, утечек, искажений, уничтожения информации в информационных и телекоммуникационных сетях и системах общегосударственного назначения. Но темпы совершенствования информационного оружия (как и любого вида атакующего вооружения) превышают темпы развития технологий защиты. Вот почему задача нейтрализации информационного оружия, парирования угрозы его применения должна рассматриваться как одна из приоритетных задач в обеспечении национальной безопасности страны.

Настоящее учебное пособие представляет собой попытку системного изложения проблем защиты информации, а также теоретических основ применения добавочных средств защиты. В пособии рассматриваются подходы к построению встроенных средств защиты современных операционных систем и приложений, выявлению причин их уязвимости на основе существующей статистики угроз. На основании этого формулируются и теоретически обосновываются общие требования к механизмам защиты, в том числе излагаются подходы к построению добавочных средств.

Целью учебного пособия является не только рассмотрение перспективных технологий и методов защиты информации от несанкционированного доступа (НСД), но и обоснование требований к системе защиты. Эти требования позволят ориентироваться на рынке средств защиты информации при выборе оптимального решения. Кроме того, в пособии немалое внимание уделено иллюстрации тех задач, которые должны решаться администратором безопасности, эксплуатирующим средства защиты. При этом следует понимать, что хорошая система защиты -- это своего рода "конструктор", в котором заложены механизмы противодействия как явным, так и скрытым угрозам информационной безопасности. Чтобы достигнуть необходимого уровня безопасности защищаемых объектов, специалист по защите информации должен не только знать и понимать возможности механизмов защиты, но и уметь их настраивать применительно к непрерывно изменяющейся статистике угроз.

Об авторах



БОРИСОВ Михаил Анатольевич

Доцент факультета военного обучения при Московском государственном университете имени М. В. Ломоносова. Квалифицированный специалист в области защиты информации. Имеет многолетний практический опыт работы в структурных

подразделениях по защите государственной тайны различных уровней. На протяжении последних нескольких лет является ведущим преподавателем курса дисциплин специальности «Защита информационных технологий» на факультете военного обучения МГУ, а также дисциплин «Правовая и организационная защита информации», «Основы менеджмента защиты информации» и «Экономика защиты информации» в ряде образовательных учреждений. Автор более 30 учебно-методических изданий и научных публикаций.



ЗАВОДЦЕВ Илья Валентинович

Кандидат технических наук, доцент. Квалифицированный специалист в области комплексной защиты информации на объектах информатизации. Имеет многолетний практический опыт работы в структурных подразделениях по защите государственной тайны различных уровней. На протяжении последних нескольких лет является ведущим преподавателем учебных дисциплин «Программно-аппаратная защита информации», «Защита информационных процессов в компьютерных системах», «Организационная защита информации», «Обеспечение безопасного электронного документооборота» в Кубанском государственном технологическом университете и в филиале Военной академии связи в г. Краснодаре. Автор более 70 научных трудов и научно-популярных статей.



ЧИЖОВ Иван Владимирович

Кандидат физико-математических наук. Квалифицированный специалист в области построения систем комплексной защиты информации как в интересах органов государственной власти, так и для различных бизнес-структур. На протяжении последних нескольких лет читает курс лекций по программно-аппаратным средствам и методам защиты информации для магистров факультета вычислительной математики и кибернетики Московского государственного университета имени М. В. Ломоносова, обучающихся по направлению «Прикладная математика и информатика». Автор 9 научных публикаций. Участник многих научно-практических конференций и семинаров в области информационной безопасности.
