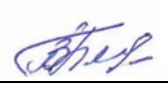
МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Тульский государственный университет»

Политехнический институт
Кафедра «Инструментальные и метрологические системы»

Утверждено на заседании кафедры
«Инструментальные и метрологические системы»
18 сентября 2024 г., протокол № 1

И.о заведующего кафедрой

 В.А. Белякова

Методические указания по проведению практических (семинарских) занятий по дисциплине (модулю)

«Информационная безопасность и технологии
искусственного интеллекта»

основной профессиональной образовательной программы высшего образования – программы бакалавриата

по направлению подготовки
27.03.04 Управление в технических системах

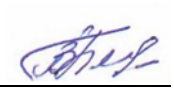
с направленностью (профилем)
Цифровые технологии в системах обеспечения качества

Форма обучения: очная

Идентификационный номер образовательной программы: 270304-01-24

Тула 2024 год

Разработчик:

Белякова В.А. к.т.н., доцент 

(ФИО, должность, ученая степень, ученое звание) *(подпись)*

Практическая работа №1.
Информационная безопасность (ИБ) в области искусственного интеллекта. Основные понятия.

Цель практической работы состоит в том, чтобы ввести в курс задач, решаемых при обеспечении ИБ в области искусственного интеллекта.

Описание практической работы

Рассматриваются основные понятия и составляющие процесса обеспечения ИБ в области искусственного интеллекта.

В качестве основных стандартов рассматриваются стандарты серии ISO 27xxx, посвященной внедрению Системы менеджмента информационной безопасности (СМИБ):

- ISO 27000 — СМИБ. Обзор и глоссарий
- ISO 27001 — СМИБ. Требования
- ISO 27002 — СМИБ. Свод практических правил для обеспечения мер ИБ
- ISO 27003 — СМИБ. Руководство по внедрению СМИБ
- ISO 27004 — СМИБ. Мониторинг, измерения, анализ и оценка
- ISO 27005 — СМИБ. Управление рисками информационной безопасности
- ISO 27018 — Свод практических правил по защите персональных данных в публичных облаках
- ISO 27031 — Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса
- ISO 27032 — Руководство по кибербезопасности
- ISO 27035 — Управление инцидентами информационной безопасности
- ISO 27036 — Информационная безопасность при взаимоотношениях с поставщиками
- ISO 27039 — Выбор, настройка и работа с системами обнаружения и предотвращения вторжений
- ISO 27043 — Принципы и процессы расследования инцидентов информационной безопасности

Основные фазы построения СМИБ по ISO 27xxx:

- Оценка необходимости и потребности компании в мерах ЗИ путем оценки рисков и моделирования угроз/нарушителей
- Внедрение и обеспечение процессов ИБ, мер защиты и иных контрмер для противодействия выявленным актуальным угрозам
- Мониторинг и регулярный пересмотр эффективности работы СМИБ
- Непрерывное совершенствование СМИБ. Ключевые компоненты СМИБ:
- Локальные нормативные акты (ЛНА)
- Сотрудники с определенными должностными обязанностями
- Процессы управления:

1. Внедрением ЛНА
2. Повышением квалификации и осведомленности сотрудников
3. Планированием

4. Внедрением мер защиты
5. Текущей деятельностью
6. Оценкой эффективности
7. Анализом со стороны руководства
8. Совершенствованием

Процессы обеспечения ИБ по стандарту ISO/IEC 27001:2013:

● процесс создания и поддержки документального обеспечения деятельности по защите информации (политики, стандарты, регламенты, процедуры, инструкции)

● процесс управления учетными записями пользователей и администраторов информационных систем

● процесс разграничения и контроля прав логического доступа к информационным системам, реализация принципа минимизации полномочий

● процесс проверки (скрининга) персонала при приеме на работу, обучение персонала принципам и политикам информационной безопасности компании, контроль выполнения требований информационной безопасности сотрудниками в процессе работы

● процесс управления активами (инвентаризация, назначение владельцев и ответственных, контроль на всех стадиях жизненного цикла активов), включая управление устройствами (стационарными, мобильными)

● процесс классификации информации по степени критичности и уровням необходимости соблюдения конфиденциальности, целостности, доступности

● процесс криптографической защиты информации при использовании, хранении и передаче

● процесс обеспечения физической безопасности и контроль физического доступа к объектам информационных систем

● операционные процессы обеспечения информационной безопасности: контроль изменений, контроль конфигураций, контроль разработки и внедрения информационных систем

● процесс защиты от вредоносного программного обеспечения

● процесс обеспечения непрерывности бизнеса и восстановления работоспособности информационных систем и данных после сбоев

● процесс аудита и мониторинга событий информационной безопасности

● процесс управления инцидентами информационной безопасности

● процесс управления уязвимостями в используемом программном обеспечении (сканирование, оценка, устранение путем обновления или наложенными средствами защиты)

● процесс обеспечения сетевой безопасности (сегментирование ЛВС, фильтрация трафика, аутентификация устройств), включая обеспечение информационной безопасности при использовании «облачных» сервисов

● процесс обеспечения информационной безопасности на всех стадиях жизненного цикла информационных систем, включая поддержку цикла безопасной разработки и внедрения программного обеспечения

● процесс контроля информационного взаимодействия с поставщиками, клиентами, подрядчиками

● процесс управления соответствием нормативным требованиям, предъявляемым к компании

● процесс проведения независимых аудитов и тестов информационной безопасности.

Каждый процесс разбит на подпроцессы для детализации требований.

Например, процесс обеспечения физической безопасности и контроль физического доступа к объектам информационных систем состоит из следующих подпроцессов:

● Создание периметра физической безопасности (защита помещений, где хранится и обрабатывается важная информация)

● Меры контроля физического доступа (СКУД, турникеты, замки и т.д.)

● Защита помещений, комнат, участков зданий

● Защита от внешних воздействий (стихийные бедствия, физические атаки)

● Контроль работы в защищенных помещениях

● Контроль зон возможного пребывания посторонних лиц (зоны погрузки/доставки должны быть ограничены)

● Физическая защита оборудования

● Защита от сбоев систем электроснабжения, вентиляции, кондиционирования

● Физическая защита структурированных кабельных систем (СКС)

● Обслуживание оборудования (очистка, охлаждение, питание)

● Защита от физического выноса оборудования из здания

● Защита оборудования за пределами контролируемых зон (бекапы, ЦОДы, удаленная работа на корпоративных ноутбуках)

● Надежное удаление информации перед утилизацией/продажей оборудования

● Защита оборудования, находящегося без присмотра (блокировка рабочих станций)

● Политика «чистого рабочего стола», защита носителей/распечаток, доступ к принтерам

Практическая работа № 2.
Основные стандарты в области обеспеченияинформационной безопасности систем искусственного интеллекта. Политика безопасности

Цель практической работы состоит в изучении основных стандартов информационной безопасности систем искусственного интеллекта.

Описание практической работы

Рассматриваются практические примеры применения стандартов информационной безопасности систем искусственного интеллекта наосновании следующих документов:

Документ NIST SP 800-53 (ревизия №5, Сентябрь 2020)

- входит в NIST Cybersecurity Framework наряду с документами по управлению рисками (NIST SP 800-39, 800-37, 800-30) и логическис ними связан;
- описывает конкретные шаги для минимизации рисков ИБ, выявленных на предыдущих этапах;
- дополнения: NIST SP 800-53A (методы оценки внедренных мер), NIST SP 800-53B (базовые уровни мер).

Меры защиты по NIST SP 800-53:

- контроль доступа
- осведомленность и обучение
- аудит и подотчетность
- оценка, авторизация и мониторинг
- управление конфигурациями
- планирование непрерывности операций идентификация и аутентификация
- реагирование на инциденты
- обслуживание систем
- защита носителей информации
- физическая безопасность и защита от стихийных бедствий
- планирование
- управление программой обеспечения информационной безопасности
- кадровая безопасность
- обработка и защита персональных данных
- оценка рисков
- приобретение систем и сервисов
- защита систем и средств коммуникации
- целостность систем и информации
- управление цепочками поставок.

Все меры защиты, описанные в стандарте NIST SP 800-53, включают в себя также и конкретные шаги по реализации соответствующей ме-

ры. Например, мера защиты «Контроль доступа» включает в себя следующие действия:

- создание политик и процедур контроля доступа
- управление учетными записями
- защиту доступа
- контроль потоков информации
- разделение и минимизацию полномочий
- контроль неудачных попыток аутентификации
- уведомление об осуществляемом мониторинге и правилах работы с информационными системами
- уведомление о предыдущих попытках аутентификации
- контроль количества параллельных сессий блокировку сессии пользователя после периода бездействия
- принудительный разрыв сессии по тайм-ауту или определенному условию
- определение списка возможных действий без прохождения идентификации или аутентификации
- использование меток безопасности и конфиденциальности
- контроль удаленного и беспроводного доступа
- контроль доступа мобильных устройств
- использование внешних систем
- предоставление общего доступа к информации
- предоставление публично доступного контента
- защита от массового извлечения данных
- принятие решений о контроле доступа
- применение контролера доступа (Reference Monitor).

Документ «CIS TOP-20 Controls»

Разработан некоммерческой организацией CIS (Center for Internet Security). Обновляется регулярно, последняя версия 7.1 (2020 г.). Кроме теоретических рекомендаций, выпускает практические документы – Benchmarks (бенчмарки, «золотые стандарты») с перечнем конкретных действий по настройке ОС, ПО, СЗИ.

Документ «CIS TOP-20 Controls» содержит 20 наиболее эффективных мер защиты (технических, организационных), разделенных на группы:

Базовые:

- Инвентаризация и контроль аппаратных активов
- Инвентаризация и контроль программных активов
- Непрерывное управление уязвимостями
- Контроль использования административных полномочий
- Защищенная настройка ПО и АО на устройствах Мониторинг и анализ журналов доступа (логов) Основные:
- Защита email-клиентов и браузеров

- Защита от ВПО
- Ограничение и контроль использования сетевых портов, сервисов и протоколов
- Возможности по восстановлению данных
- Защищенная настройка сетевых устройств (межсетевые экраны, маршрутизаторы, коммутаторы)
- Защита информационного периметра
- Защита данных
- Контролируемый доступ на основе принципа служебной необходимости
- Контроль беспроводного доступа
- Мониторинг и контроль учетных записей Организационные:
- Программа повышения осведомленности и обучение сотрудников
- Безопасность прикладного ПО (безопасная разработка)
- Управление и реагирование на инциденты
- Тесты на проникновение и тесты «Red Team»

Все меры защиты содержат в себе 5-10 подпунктов с конкретизацией меры. Например, мера №14 «Контролируемый доступ на основе принципа служебной необходимости» состоит из подпунктов:

- Сегментация ЛВС на основе важности данных, обрабатываемых в каждом из сегментов (VLAN)
- Фильтрация трафика между сегментами сети
- Запрет на взаимодействие между клиентскими устройствами (для блокировки распространения ВПО) Шифрование всей важной информации в процессе передачи
- Автоматизированный поиск важной информации в сети (для обновления списка защищаемых активов)
- Защита информации с применением списков контроля доступа (ACL, Access Control List)
- Контроль доступа к информации (например, с применением DLP)
- Шифрование всей важной информации в процессе хранения
- Детальное логирование всех фактов доступа и изменения важной информации

Этапы выстраивания системы управления информационной безопасностью:

- Изучение бизнеса компании, включая бизнес-процессы, используемые технологии, средства защиты
- Выявление рисков, угроз, применимых регуляторных норм
- Выбор наиболее подходящих стандартов, рекомендаций и лучших практик для выстраивания процессов ИБ конкретно в данной компа-

нии

- Составление списка мер защиты (организационные, технические, физические), которые закрывают выявленные риски и угрозы
- Дополнение списка мерами, которые продиктованы регуляторными нормами
- Разработка и утверждение локальной (внутренней) нормативной документации (сначала политики и стандарты ИБ, затем по мере необходимости регламенты, процедуры, инструкции – с индексами документов, грифом, сквозной нумерацией, историей изменений, версионностью, списком согласовавших и утвердивших)

Повторный анализ имеющихся СЗИ – реализуют ли они все выявленные необходимые меры защиты?

- Выбор новых СЗИ и/или модернизация старых. Экономическое обоснование затрат (инвестиций) в СЗИ. Приобретение СЗИ
- Набор сотрудников в подразделение защиты информации (для работы с конкретными технологиями и средствами ИБ)
- Внедрение СЗИ (силами подрядчиков или самостоятельно), первичная настройка
- Контроль выполнения ЛНА с помощью СЗИ. Контроль минимизации рисков до заданного уровня (снижение количества инцидентов). Тюнинг СЗИ
- Непрерывное улучшение, охват все больших объектов бизнеса и ИТ-инфраструктуры

Экономическое обоснование затрат (инвестиций) в СЗИ. Приобретение СЗИ

- CAPEX – capital expenditure, капитальные расходы (сервер, ПК, коробочное СЗИ)
- OPEX – operational expenditure, операционные расходы (облако, аренда ЦОД, использование СЗИ по подписке)
- ROSI – Return on Security Investment, возврат инвестиций в безопасность – экономическая эффективность СЗИ. Если ROSI > 1, то вложение в СЗИ оправдано.

ROSI = (ARO*SLE*MF – TCO) / TCO

ARO - annualized rate of occurrence, среднее количество инцидентов в год в соответствии со статистическими данными

SLE - single loss expectancy, ожидаемые разовые потери, т.е. «стоимость» одного инцидента

MF - mitigation factor, фактор снижения угрозы с помощью СЗИ (в %) TCO - total cost of ownership, совокупная стоимость владения СЗИ,

включающая в себя стоимость самого СЗИ, затрат на внедрение, техподдержку вендора, регулярные обновления, зарплату администрирующего СЗИ персонала.

Пример:

DDoS-атаки происходят 10 раз в год, ущерб от одной DDoS-атаки = 1000000 рублей, MF = 90% по заявлению производителя анти-DDoS решения, TCO = (2000000 рублей само СЗИ + 1500000 рублей годовая з/п администратора ИБ + внедрение 300000 рублей) = 3800000 руб.

ROSI = (10*1000000*0.9 – 3800000) / 3800000 = 1.37.

Практическая работа № 3

Основные виды сетевых и компьютерных угроз.Средства и методы защиты от сетевых компьютерных угроз

Цель практической работы состоит в рассмотрении основных видовсетевых и компьютерных угроз и методов их нейтрализации**.**

Описание практической работы

Рассматриваются на практике основные виды сетевых и компьютерныхугроз:

1. Анализ сетевого трафика

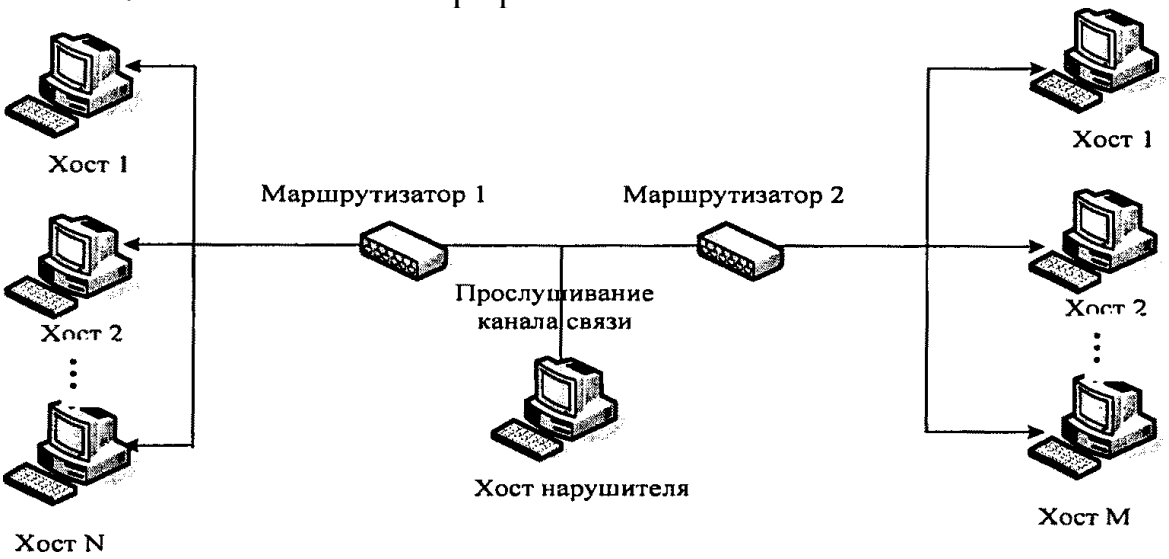


Схема реализации угрозы "Анализ сетевого трафика"

Эта угроза реализуется с помощью специальной программы-анализатора пакетов (sniffer), перехватывающей все пакеты, передаваемые по сегменту сети, и выделяющей среди них те, в которых передаются идентификатор пользователя и его пароль. В ходереализации угрозы нарушитель изучает логику работы сети - то есть стремится получить однозначное соответствие событий, происходящих в системе, и команд, пересылаемых при этом хостами, в момент появления данных событий. В дальнейшем это позволяет злоумышленнику на основе задания соответствующих команд получить, например, привилегированные права на действия в системе или расширить свои полномочия в ней, перехватить поток передаваемых данных, которыми обмениваются компоненты сетевой операционной системы, для извлечения конфиденциальной или

идентификационной информации (например, статических паролей пользователей для доступа к удаленным хостам по протоколам FTP и TELNET, не предусматривающим шифрование), ее подмены, модификации и т.п.

2. Сканирование сети.

Сущность процесса реализации угрозы заключается в передаче запросов сетевым службам хостов ИСПДн и анализе ответов от них. Цель - выявление используемых протоколов, доступных портов сетевых служб, законов формирования идентификаторов соединений, определение активных сетевых сервисов, подбор идентификаторов и паролей пользователей.

3. Угроза выявления пароля.

Цель реализации угрозы состоит в получении НСД путем преодоления парольной защиты. Злоумышленник может реализовывать угрозу с помощью целого ряда методов, таких как простой перебор, перебор с использованием специальных словарей, установка вредоносной программы для перехвата пароля, подмена доверенного объекта сети (IP-spoofing) и перехват пакетов (sniffing). В основном для реализации угрозы используются специальные программы, которые пытаются получить доступ к хосту путем последовательного подбора паролей. В случае успеха, злоумышленник может создать для себя "проход" для будущего доступа, который будет действовать, даже если на хосте изменить пароль доступа.

4. Подмена доверенного объекта сети и передача по каналам связи сообщений от его имени с присвоением его прав доступа.

Такая угроза эффективно реализуется в системах, где применяются нестойкие алгоритмы идентификации и аутентификации хостов, пользователей и т.д. Под доверенным объектом понимается объект сети (компьютер, межсетевой экран, маршрутизатор и т.п.), легально подключенный к серверу.

Могут быть выделены две разновидности процесса реализации указанной угрозы: с установлением и без установления виртуального соединения.

Процесс реализации с установлением виртуального соединения состоит в присвоении прав доверенного субъекта взаимодействия, что позволяет нарушителю вести сеанс работы с объектом сети от имени доверенного субъекта. Реализация угрозы данного типа требует преодоления системы идентификации и аутентификации сообщений (например, атака rsh-службы UNIX-хоста).

Процесс реализации угрозы без установления виртуального соединения может иметь место в сетях, осуществляющих идентификацию передаваемых сообщений только по сетевому адресу отправителя. Сущность заключается в передаче служебных сообщений от имени сетевых управляющих устройств (например, от имени маршрутизаторов) об изменении маршрутно-адресных данных. При этом необходимо иметь в виду, что единственными идентификаторамиабонентов и соединения (по протоколу TCP) являются два 32-битных параметра Initial Sequence Number - ISS (номер последовательности) и Acknowledgment Number - ACK (номер подтверждения). Следовательно, для формирования ложного TCP-пакета нарушителю необходимо знать текущие идентификаторы для данного соединения -ISSa и ISSb, где:

ISSa - некоторое численное значение, характеризующее порядковый номер отправляемого TCP-пакета, устанавливаемого TCP-соединения, инициированного хостом A;

ISSb - некоторое численное значение, характеризующее порядковый номер отправляемого TCP-пакета, устанавливаемого TCP-соединения, инициированного хостом B.

Значение ACK (номера подтверждения установления TCP- соединения) определяется как значение номера, полученного от респондента ISS (номер последовательности) плюс единица ACKb = ISSa + 1.

В результате реализации угрозы нарушитель получает права доступа, установленные его пользователем для доверенного абонента,к техническому средству ИСПДн - цели угроз.

5. Навязывание ложного маршрута сети.

Данная угроза реализуется одним из двух способов: путем внутрисегментного или межсегментного навязывания. Возможность навязывания ложного маршрута обусловлена недостатками, присущими алгоритмам маршрутизации (в частности, из-за проблемы идентификации сетевых управляющих устройств), в результате чего можно попасть, например, на хост или в сеть злоумышленника, где можно войти в операционную среду технического средства в составе ИСПДн. Реализация угрозы основывается на несанкционированном использовании протоколов маршрутизации (RIP, OSPF, LSP) и управления сетью (ICMP, SNMP) для внесения изменений в маршрутно-адресные таблицы. При этом нарушителю необходимо

послать от имени сетевого управляющего устройства (например, маршрутизатора) управляющее сообщение.

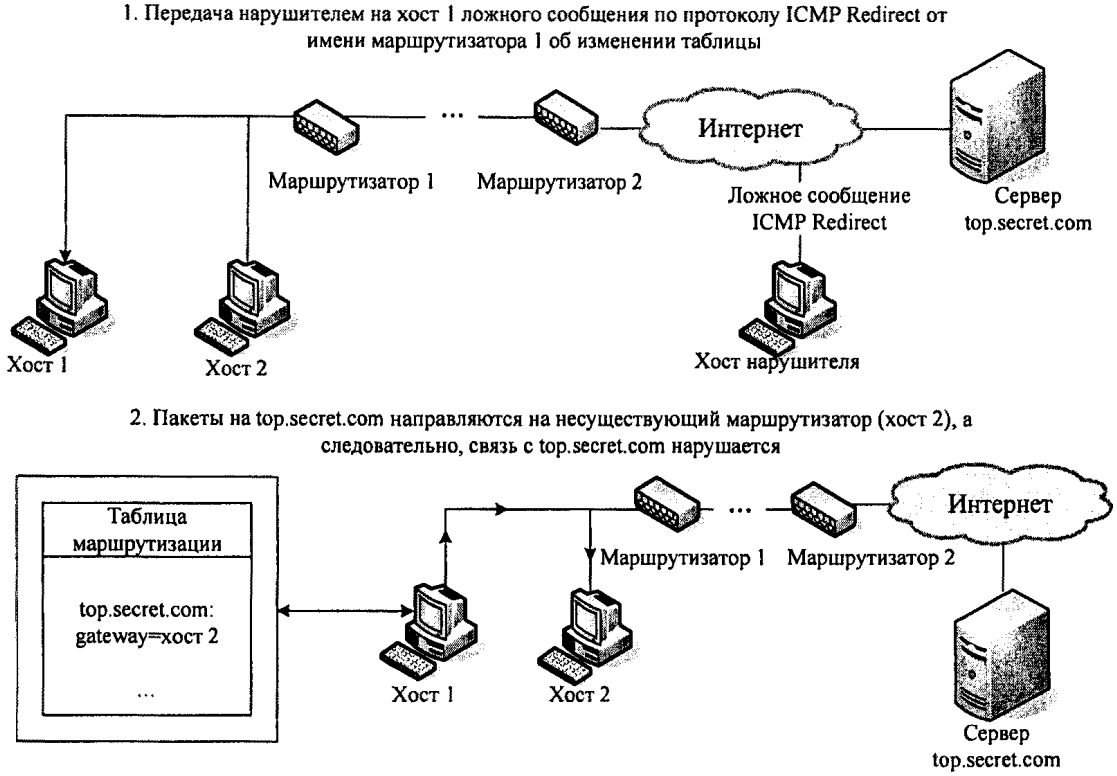


Схема реализации атаки "Навязывание ложного маршрута" (внутрисегментное) с использованием протокола ICMP с целью нарушения связи

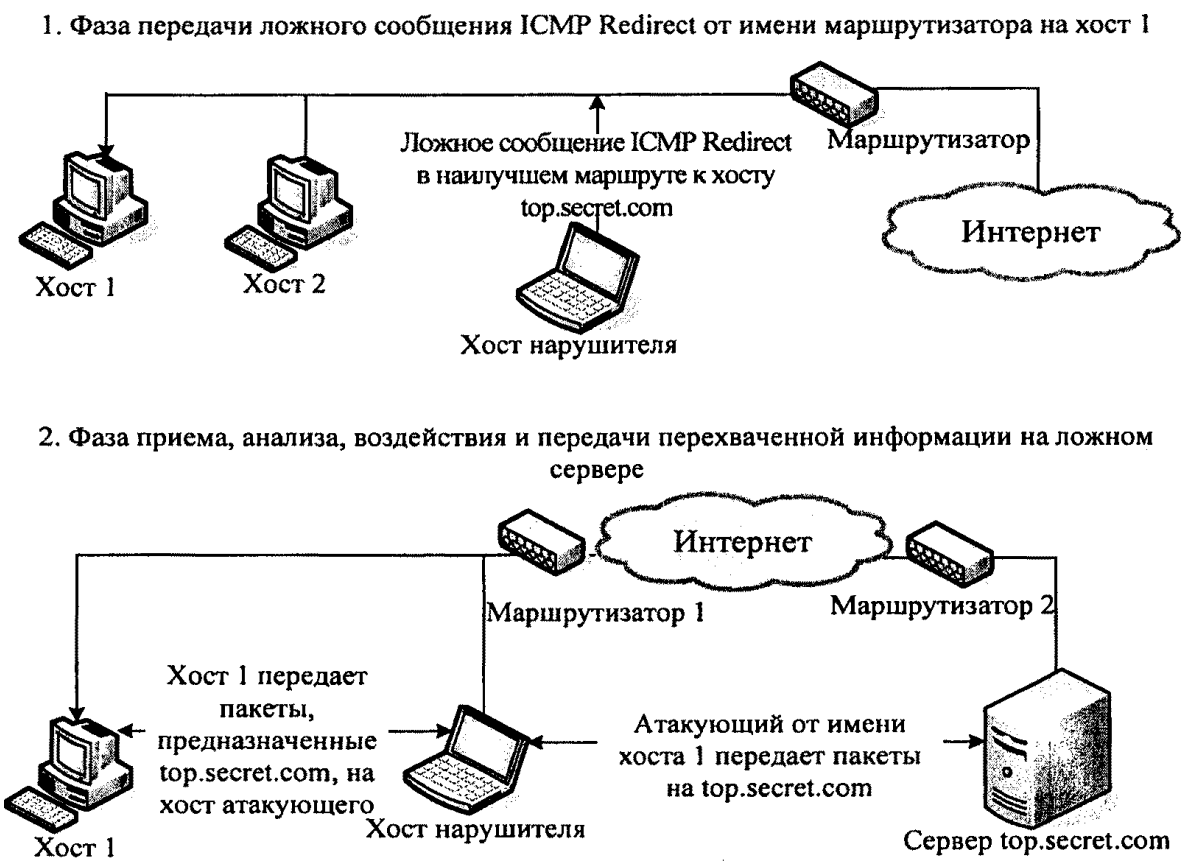


Схема реализации угрозы "Навязывание ложного маршрута" (межсегментное) с целью перехвата трафика

6. Внедрение ложного объекта сети.

Эта угроза основана на использовании недостатков алгоритмов удаленного поиска. В случае, если объекты сети изначально не имеют адресной информации друг о друге, используются различные протоколы удаленного поиска (например, SAP в сетях Novell NetWare; ARP, DNS, WINS в сетях со стеком протоколов TCP/IP), заключающиеся в передаче по сети специальных запросов и получении на них ответов с искомой информацией. При этом существует возможность перехвата нарушителем поискового запроса и выдачи на него ложного ответа, использование которого приведет к требуемому изменению маршрутно-адресных данных.

В дальнейшем весь поток информации, ассоциированный с объектом-жертвой, будет проходитьчерез ложный объект сети.

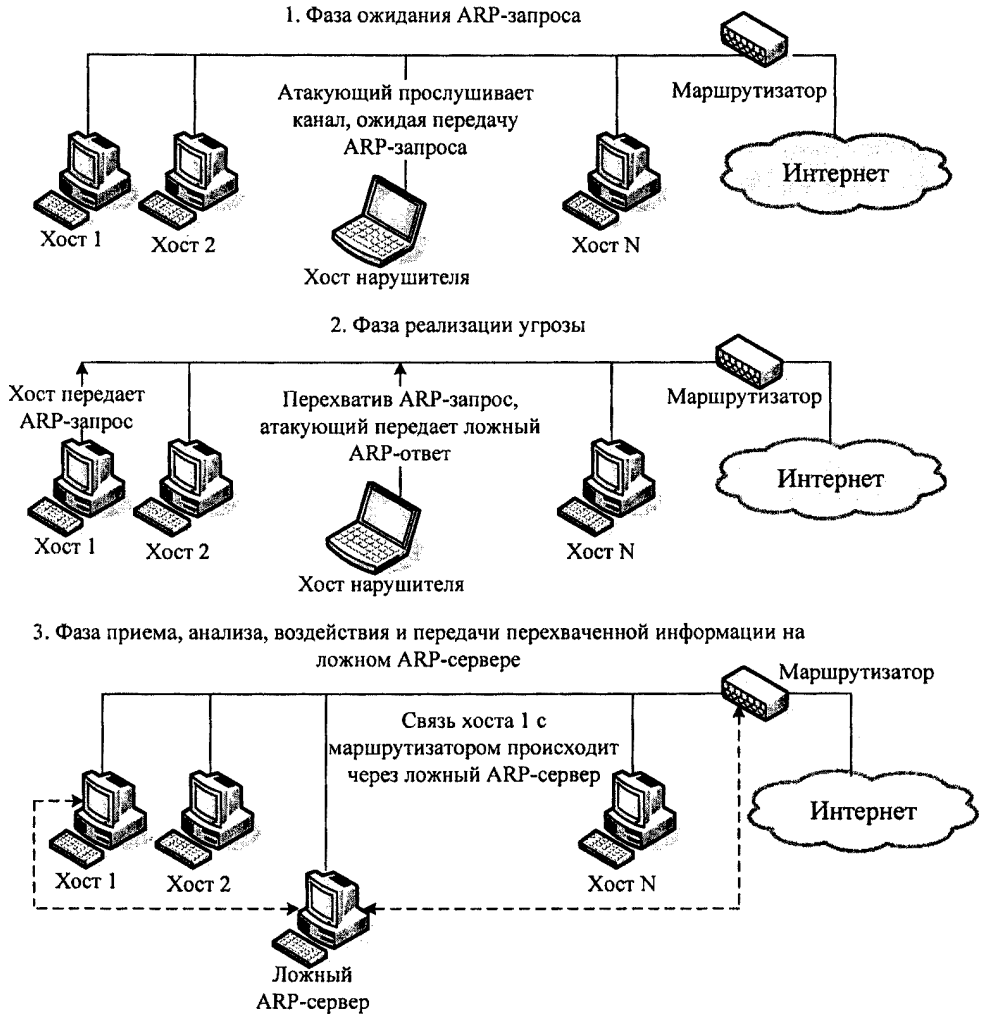


Схема реализации угрозы "Внедрение ложногоARP-сервера"

7. Отказ в обслуживании.

Эти угрозы основаны на недостатках сетевого программного обеспечения, его уязвимостях, позволяющих нарушителю создавать условия, когда операционная система оказывается не в состоянии обрабатывать поступающие пакеты.

Могут быть выделены несколько разновидностей таких угроз:

а) скрытый отказ в обслуживании, вызванный привлечением части ресурсов ИСПДн на обработку пакетов, передаваемых злоумышленником со снижением пропускной способности каналов связи, производительности сетевых устройств, нарушением требований ко времени обработки запросов. Примерами реализации угроз подобного рода могут служить: направленный шторм эхозапросов по протоколу ICMP (Ping flooding), шторм запросов на

установление TCP-соединений (SYN-flooding), шторм запросов к FTP-серверу;

б) явный отказ в обслуживании, вызванный исчерпанием ресурсов ИСПДн при обработке пакетов, передаваемых злоумышленником (занятие всей полосы пропускания каналов связи, переполнение очередей запросов на обслуживание), при котором легальные запросы не могут быть переданы через сеть из-за недоступности среды передачи либо получают отказ в обслуживании ввиду переполнения очередей запросов, дискового пространства памяти и т.д. Примерами угроз данного типа могут служить шторм широковещательных ICMP- эхо-запросов (Smurf), направленный шторм (SYN-flooding), шторм сообщений почтовому серверу (Spam);

в) явный отказ в обслуживании, вызванный нарушением логической связности между техническими средствами ИСПДн при передаче нарушителем управляющих сообщений от имени сетевых устройств, приводящих к изменению маршрутно-адресных данных (например, ICMP Redirect Host, DNS-flooding) или идентификационной и аутентификационной информации;

г) явный отказ в обслуживании, вызванный передачей злоумышленником пакетов с нестандартными атрибутами (угрозы типа "Land", "TearDrop", "Bonk", "Nuke", "UDP-bomb") или имеющих длину, превышающую максимально допустимый размер (угроза типа "Ping Death"), что может привести к сбою сетевых устройств, участвующих в обработке запросов, при условии наличия ошибок в программах, реализующих протоколы сетевого обмена.

Результатом реализации данной угрозы может стать нарушение работоспособности соответствующей службы предоставления удаленного доступа к ПДн в ИСПДн, передача с одного адреса такого количества запросов на подключение к техническому средству в составе ИСПДн, какое максимально может "вместить" трафик (направленный "шторм запросов"), что влечет за собой переполнение очереди запросов и отказ одной из сетевых служб или полную остановку компьютера из-за невозможности системы заниматься ничем другим, кроме обработки запросов.

8. Удаленный запуск приложений.

Угроза заключается в стремлении запустить на хосте ИСПДн различные предварительно внедренные вредоносные программы: программы-закладки, вирусы, "сетевые шпионы", основная цель которых - нарушение конфиденциальности, целостности, доступностиинформации и полный контроль за работой хоста. Кроме того, возможен несанкционированный запуск прикладных программ пользователей для несанкционированного получения необходимых нарушителю данных, для запуска управляемых прикладной программой процессов и др.

Выделяют три подкласса данных угроз:

1) распространение файлов, содержащих несанкционированный исполняемый код;

2) удаленный запуск приложения путем переполнения буфера приложений-серверов;

3) удаленный запуск приложения путем использования возможностей удаленного управления системой, предоставляемых скрытыми программными и аппаратными закладками либо используемыми штатными средствами.

Типовые угрозы первого из указанных подклассов основываются наактивизации распространяемых файлов при случайном обращении к ним. Примерами таких файлов могут служить: файлы, содержащие исполняемый код в виде макрокоманд (документы Microsoft Word, Excel и т.п.); html-документы, содержащие исполняемый код в виде элементов ActiveX, Java-апплетов, интерпретируемых скриптов (например, тексты на JavaScript); файлы, содержащие исполняемые коды программ. Для распространения файлов могут использоваться службы электронной почты, передачи файлов, сетевой файловой системы.

При угрозах второго подкласса используются недостатки программ, реализующих сетевые сервисы (в частности, отсутствие контроля переполнения буфера). Настройкой системных регистров иногда удается переключить процессор после прерывания, вызван-

ного переполнением буфера, на исполнение кода, содержащегося за

границей буфера. Примером реализации такой угрозы может служить внедрение широко известного "вируса Морриса".

При угрозах третьего подкласса нарушитель использует возможности удаленного управления системой, предоставляемые скрытыми компонентами (например, "троянскими" программами типаBack Orifice, Net Bus) либо штатными средствами управления и администрирования компьютерных сетей (Landesk Management Suite, Managewise, Back Orifice и т.п.). В результате их использования удается добиться удаленного контроля над станцией в сети.

Схематично основные этапы работы этих программ выглядят следующим образом:

- инсталляция в памяти;
- ожидание запроса с удаленного хоста, на котором запущенаклиент-программа, и обмен с ней сообщениями о готовности;
- передача перехваченной информации клиенту илипредоставление ему контроля над атакуемым компьютером.

Практическая работа № 4.

Методы анализа рисков. Понятиеуязвимости. Классификация угроз. Методы оценки ущерба от реализации угроз информационной безопасности систем искусственного интеллекта.

Целью работы является ознакомление с общими принципами анализа рисков и определения уязвимостей.

Задачи:

1. Провести анализ уязвимостей.
2. Оценить негативный эффект от обнаруженных уязвимостей.
3.

Теоретические положения

Теоретические положения отражены в нормативной документацииФСТЭК России.

Порядок выполнения работы

1. Осуществить выбор средства анализа защищенности и поиска уязвимостей.
2. Произвести сканирование выделенных узлов на уязвимости.
3. Проанализировать отчет по итогам сканирования.
4. Оценить риски и ущерб от реализации выявленных уязвимостей.
5. Предложить план устранения найденных уязвимостей.

Варианты заданий

Выполнить этапы анализа уязвимостей на виртуальных машинах соследующими ОС:

1. Windows 10
2. Windows 8.1
3. Windows 7
4. Windows Server 2012.
5. Windows Server 2016.

Требования и состав отчёта

1. Отчёт должен быть выполнен на листах размера А4.
2. Отчёт должен начинаться с титульного листа с названием вуза и факультета, номером и названием лабораторной работы, вариантом,

ФИО студента, № группы, ФИО преподавателя, городом и годом.

3. В отчёте нужно кратко описать задание, показать основные этапы решения задачи, сформулировать выводы.

4. Отчёт предоставить в бумажном или электронном виде (записать нафлэш-накопитель и продублировать на электронную почту).

Вопросы и задания

1. Описать связь между угрозами и уязвимостями.
2. Привести основные методы анализа рисков.
3. привести основные методы оценки ущерба от реализации уязвимостей.

При защите отчёта надо уметь отвечать на вопросы по постановке задачи, этапам ее решения, использованным инструментам, формулам, справочникам и нормативным документам.

Практическая работа № 5.
Специализированные программно- аппаратные средства защиты информации для систем искусственногоинтеллекта. Основные направления применения криптографических технологий при защите систем искусственного интеллекта

Целью работы является ознакомление с общими принципами применения средств защиты информации для систем искусственного интеллекта.

Задачи:

1. Провести анализ СЗИ.
2. Выбрать СЗИ, необходимые для рассматриваемой задачи.
3. Рассмотреть основные аспекты применения СКЗИ.

Теоретические положения

Теоретические положения отражены в нормативной документации ФСТЭК России.

Порядок выполнения работы

1. Рассмотрение вариантов применения СЗИ для данной задачи.
2. Выбор критериев для отбора СЗИ.
3. Выбор СЗИ с указанием места их применения на схеме комплексатехнических средств.
4. Выбор СКЗИ для решения задачи обеспечения ИБ.

Варианты заданий

Выполнить этапы выбора СЗИ по требованиям:

1. Приказа № 17 от 13.02.2013 ФСТЭК России.
2. Приказа № 21 от 18.02.2013 ФСТЭК России.
3. К обеспечению безопасности АС.
4. К обеспечению безопасности КИИ.

Требования и состав отчёта

1. Отчёт должен быть выполнен на листах размера А4.
2. Отчёт должен начинаться с титульного листа с названием вуза и факультета, номером и названием лабораторной работы, вариантом, ФИО студента, № группы, ФИО преподавателя, городом и годом.
3. В отчёте нужно кратко описать задание, показать основные этапы решения задачи, сформулировать выводы.
4. Отчёт предоставить в бумажном или электронном виде (записать нафлэш-накопитель и продублировать на электронную почту).

Вопросы и задания

1. Повторить и закрепить принципы формулирования требований к мерам защиты.
2. Повторить и закрепить требования к применению СКЗИ.

Практическая работа № 6
Тема: «Особенности защиты информации в базах данных»

Цель работы: Закрепление теоретического материала по изучению особенностей защиты информации в базах данных.

Изучение способов и систем защиты информации в базах данных.

Приборы и оборудование:

Персональный компьютер ОС MS Windows 7 (MS Windows 10), MS Office, Браузер Microsoft Internet Explorer (Edge)

Пояснения к работе и задание:

Базы данных рассматриваются как надежное хранилище структурированных данных, снабженное специальным механизмом для их эффективного использования в интересах пользователей (процессов). Таким механизмом является система управления базами данных (СУБД). Под системой управления базой данных понимаются программные или аппаратнопрограммные средства, реализующие функции управления данными, такие как: просмотр, сортировка, выборка, модификация, выполнение операций определения статистических характеристик и т.п. Базы данных размещаются:

- на компьютерной системе пользователя;
- на специально выделенной ЭВМ(сервере).

Как правило, на компьютерной системе пользователя размещаются личные или персональные базы данных, которые обслуживают процессы одного пользователя.

В вычислительных сетях базы данных размещаются на серверах. В локальных и корпоративных сетях, как правило, используются централизованные базы данных. В таких сетях серверы размещаются на различных объектах сети. В качестве серверов часто используются специализированные ЭВМ, приспособленные к хранению больших объемов данных, обеспечивающие сохранность и доступность информации, а также оперативность обработки поступающих запросов. В централизованных базах данных проще решаются проблемы защиты информации от преднамеренных угроз, поддержания актуальности и непротиворечивости данных. Достоинством распределенных баз данных, при условии дублирования данных, является их высокая защищенность от стихийных бедствий, аварий, сбоев технических средств, а также диверсий.

Защита информации в БД, в отличии от защиты в файлах, имеет и свои особенности:

- необходимость учета функционирования СУБД при выборе механизмов защиты;
- разграничение доступа к информации реализуется не на уровне файлов, а на уровне частей БД.

При создании средств защиты информации в БД необходимо учитывать взаимодействие этих средств не только с ОС, но и с СУБД. При этом возможно встраивание механизмов защиты в СУБД или использование их в виде отдель-

ных компонент. Для большинства СУБД придание им дополнительных функций возможно только на этапе разработки СУБД. В эксплуатируемые СУБД дополнительные компоненты могут быть внесены путем расширения или модификации языка управления. Таким путем можно осуществлять наращивание возможностей, например, в СУБД CA-Clipper 5.0.

В современных БД довольно успешно решаются задачи разграничения доступа, поддержания физической целостности и логической сохранности данных. Алгоритмы разграничения доступа к записям и даже к полям записей в соответствии с полномочиями пользователя хорошо отработаны, и преодолеть эту защиту злоумышленник может лишь с помощью фальсификации полномочий или внедрения вредительских программ. Разграничение доступа к файлам БД и к частям БД осуществляется СУБД путем установления полномочий пользователей и контроля этих полномочий при допуске к объектам доступа.

Полномочия пользователей устанавливаются администратором СУБД. Обычно стандартным идентификатором пользователя является пароль, передаваемый в зашифрованном виде. В распределенных компьютерных системах процесс подтверждения подлинности пользователя дополняется специальной процедурой взаимной аутентификации удаленных процессов. БД, содержащих конфиденциальную информацию, хранятся на внешних запоминающих устройствах в зашифрованном виде.

Физическая целостность БД достигается путем использования отказоустойчивых устройств, построенных, например, на технологии RAID. Логическая сохранность данных означает невозможность нарушения структуры модели данных. Современные СУБД обеспечивает такую логическую целостность и непротиворечивость на этапе описания модели данных.

В БД, работающих с конфиденциальной информацией, необходимо дополнительно использовать криптографические средства закрытия информации. Для этой цели используется шифрование, как с помощью единого ключа, так и с помощью индивидуальных ключей пользователей. Применение шифрования с индивидуальными ключами повышает надежность механизма разграничения доступа, но существенно усложняет управление.

Возможны два режима с зашифрованными БД. Наиболее простым является такой порядок работы с закрытыми данными, при котором для выполнения запроса необходимый файл или часть файла расшифровывается на внешнем носителе, с открытой информацией производятся необходимые действия, после чего информация на внешнем запоминающем устройстве(ВЗУ) снова зашифровывается. Достоинством такого режима является независимость функционирования средств шифрования и БУБД, которые работают последовательно друг за другом. В то же время сбой или отказ в системе может привести к тому, что на ВЗУ часть БД останется записанной в открытом виде.

Второй режим предполагает возможность выполнения СУБД запросов пользователей без расшифрования информации на ВЗУ. Поиск необходимых файлов, записей, полей, групп полей не требует расшифрования. Расшифрование производится в ОП непосредственно перед выполнением конкретных действий с данными. Такой режим возможен, если процедуры шифрования встрое-

ны в СУБД. При этом достигается высокий уровень защиты от несанкционированного доступ, но реализация режима связана с усложнением СУБД. Придание СУБД возможности поддержки такого режима работы осуществляется, как правило, на этапе разработки СУБД.

При построении защиты БД необходимо учитывать ряд специфических угроз безопасности информации, связанных с концентрацией в БД большого количества разнообразной информации, а также с возможностью использования сложных запросов обработки данных. К таким угрозам относятся:

- инференция;
- агрегирование;
- комбинация разрешенных запросов для получения закрытых данных.

Под инференцией понимается получение конфиденциальной информации из сведений с меньшей степенью конфиденциальности путем умозаключений. Если учитывать, что в базах данных хранится информация, полученная из различных источников в разное время, отличающаяся степенью обобщенности, то аналитик может получить конфиденциальные сведения путем сравнения, дополнения и фильтрации данных, к которым он допущен. Кроме того, он обрабатывает информацию, полученную из открытых баз данных, средств массовой информации, а также используются просчеты лиц, определяющих степень важности и конфиденциальности отдельных явлений, процессов, фактов, полученных результатов. Такой способ получения конфиденциальных сведений, например, по материалам средств массовой информации, используется давно, и показал свою эффективность.

Близким к инференции является другой способ добывания конфиденциальных сведений-агрегирование. Под агрегированием понимается способ получения более важных сведений по сравнению с важностью тех отдельно взятых данных, на основе которых и получаются эти сведения. Так, сведения о деятельности одного отделения или филиала корпорации обладают определенным весом. Данные же за всю корпорацию имеют куда большую значимость.

Если инференция и агрегирование являются способами добывания информации, которые применяются не только в отношении баз данных, то способ специального комбинирования запросов используется только при работе с базами данных. Использование сложных, а также последовательности простых логически связанных запросов позволяет получать данные, к которым доступ пользователю закрыт. Такая возможность имеется, прежде всего, в базах данных, позволяющих получать статистические данные. При этом отдельные записи, поля, (индивидуальные данные) являются закрытыми. В результате запроса, в котором могут использоваться логические операции AND, OR, NOT, пользователь может получить такие величины как количество записей, сумма, максимальное или минимальное значение. Используя сложные перекрестные запросы и имеющуюся в его распоряжении дополнительную информацию об особенностях интересующей записи (поля), злоумышленник путем последовательной фильтрации записей может получить доступ к нужной записи (полю).

Противодействие подобным угрозам осуществляется следующими методами:

 блокировка ответа при неправильном числе запросов;
 искажение ответа путем округления и другой преднамеренной коррекции данных;
 разделение баз данных;
 случайный выбор записи для обработки;
 контекстно-ориентированная защита;
 контроль поступающих запросов.

Метод блокировки ответа при неправильном числе запросов предполагает отказ в выполнении запроса, если в нем содержится больше определенного числа совпадающих записей из предыдущих запросов. Таким образом, данный метод обеспечивает выполнение принципа минимальной взаимосвязи вопросов. Этот метод сложен в реализации, так как необходимо запоминать и сравнивать все предыдущие запросы.

Метод коррекции заключается в незначительном изменении точного ответа на запрос пользователя. Для того, чтобы сохранить приемлемую точность статистической информации, при меняется так называемый свопинг данных. Сущность его заключается во взаимном обмене значений полей записи, в результате чего все статистики i-го порядка, включающие i атрибутов, оказываются защищенными для всех i, меньших или равных некоторому числу. Если злоумышленник сможет выявить некоторые данные, то он не сможет определить, к какой конкретно записи они относятся.

Применяется также метод разделения баз данных на группы. В каждую группу может быть включено не более определенного числа записей. Запросы разрешены к любому множеству групп, но запрещаются к подмножеству записей из одной группы. Применение этого метода ограничивает возможности выделения данных злоумышленником на уровне не ниже группы записей. Метод разделения баз данных не нашел широкого применения из-за сложности получения статистических данных, обновления и реструктуризации данных.

Эффективным методом противодействия исследованию баз данных является метод случайного выбора записей для статистической обработки. Такая организация выбора записей не позволяет злоумышленнику проследить множество запросов.

Сущность контекстно-ориентированной защиты заключается в назначении атрибутов доступа (чтение, вставка, удаление, обновление, управление и т. д.) элементам базы данных (записям, полям, группам полей) в зависимости от предыдущих запросов пользователя.

Например, пусть пользователю доступны в отдельных запросах поля: «идентификационные номера» и «фамилии сотрудников», а также «идентификационные номера» и «размер заработной платы». Сопоставив ответы по этим запросам, пользователь может получить закрытую информацию о заработной плате конкретных работников. Для исключения такой возможности пользователю следует запретить доступ к полю «идентификатор сотрудника» во втором запросе, если он уже выполнил первый запрос.

Одним из наиболее эффективных методов защиты информации в базах данных является контроль поступающих запросов на наличие «подозритель-

ных» запросов или комбинации запросов. Анализ подобных попыток позволяет выявить возможные каналы получения несанкционированного доступа к закрытым данным.

Ход выполнения лабораторной работы:

1. Изучить приведенный в методическом описании к лабораторной работе материал.
2. Выполнить практическое ознакомление с разделами с применением возможностей лаборатории.
3. Оформить отчет в установленной форме по разделам.
4. Ответить на контрольные вопросы.
5. Представить результаты работы преподавателю.

Контрольные вопросы:

1. В чем заключается особенность размещения баз данных?
2. В чем заключаются особенности защиты информации в базах данных?
3. Какие задачи решаются в рамках реализации защиты баз данных?
4. Перечислите режимы работы с защищенными базами данных.
5. Перечислите виды угроз информации, размещенной в базах данных.
6. Какие виды противодействия угрозам информации в базах данных Вы знаете?

Практическая работа № 7
Тема: «Шифрование информации методом простой замены»

Цель работы: 1. Закрепление теоретического материала на тему «Шифрование информации методом простой замены».

2. Получение шифротекста по исходным данным.

3. Получение исходного текста по заданному шифротексту и ключу.

Пояснения к работе:

Сущность методов замены (подстановки) заключается в замене символов исходной информации, записанных в одном алфавите, символами из другого алфавита по определенному правилу.

Самым простым является метод прямой замены. Символам Soi исходного алфавита Ao, с помощью которых записывается исходная информация, однозначно ставятся в соответствие символы S1i шифрующего алфавита Ai. В простейшем случае оба алфавита могут состоять из одного и того же набора символов. Например, оба алфавита могут содержать буквы алфавита кириллица.

Задание соответствия между символами обоих алфавитов осуществляется с помощью преобразования числовых эквивалентов символов исходного текста To, длиной - K символов, по определенному алгоритму.

Алгоритм моноалфавитной замены может быть представлен в виде последовательности шагов.

Шаг 1. Формирование числового кортежа Loh путем замены каждого символа Soi To (i=l,K), представленного в исходном алфавите Ao размера [lxR], на число hoi(soi), соответствующее порядковому номеру символа soi в алфавите Ao.

Шаг 2. Формирование числового кортежа L1h путем замены каждого числа кортежа Loh на соответствующее число h1i кортежа L1h, вычисляемое по формуле:

$$h_{1i} = (k_1 \times h_{0i}(s_{0i}) + k_2)(\mathrm{mod}\ R),$$

где ki - десятичный коэффициент; к2 - коэффициент сдвига. Выбранные коэффициенты K1, K2 должны обеспечивать однозначное соответствие чисел hoi и h1i, а при получении h1i = 0 выполнить замену h1i = R.

Шаг 3. Получение шифротекста T1 путем замены каждого числа h1i(s1i) кортежа L1h соответствующим символом s1i Ti (i=l,K) алфавита шифрования A1 размера [1XR].

Шаг 4. Полученный шифротекст разбивается на блоки фиксированной длины b. Если последний блок оказывается неполным, то в конец блока помещаются специальные символы-заполнители (например, символ *).

Пример. Исходными данными для шифрования являются:

T0 = <МЕТОД_ШИФРОВАНИЯ>;

Ao = <АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩ ЪЫЬЭЮЯ >;

A1 = <ОРЩЬЯТЭ_ЖМЧХАВДЫФКСЕЗПИЦГНЛЪШБУЮ>;

R=32; k1=3; k2=15, b=4.

Пошаговое выполнение алгоритма приводит к получению сле¬дующих результатов.

Шаг1. L0h = <12,6,18,14,5,32,24,9,20,1б,14,3,1,13,9,31>.

Шаг 2. L1h = <19,1,5,25,30,15,23,10,11,31,25,24,18,22,10,12>.

Шаг 3. T1 =<С О Я Г Б Д И М Ч У Г Ц К П М Х >.

Шаг4. T2 = <СОЯГ БДИМ ЧУГЦ КПМХ>.

При расшифровании сначала устраняется разбиение на блоки. Получается непрерывный шифротекст Ti длиной К символов. Расшифрование осуществляется путем решения целочисленного уравнения:

$$k_1 h_{0i} + k_2 = nR + h_{1i},$$

При известных целых величинах ki, k2, h1i и R величина hoi вычисляется методом перебора n.

Последовательное применение этой процедуры ко всем символам шифротекста приводит к его расшифрованию.

По условиям приведенного примера может быть построена таблица замены, в которой взаимозаменяемые символы располагаются в одном столбце (табл. 1).

s_{0i}	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш								
h_{0i}	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24								
s_{1i}	К	З	Ц	Л	Б	О	Ь	Э	М	А	Ы	С	П	Г	Ъ	У	Р	Я	_	Ч	В	Ф	Е	И								
h_{1i}	18	21	24	27	30	1	4	7	10	13	16	19	22	25	28	31	2	5	8	11	14	17	20	23								

s_{0i}	Щ	Ъ	Ы	Ь	Э	Ю	Я	_
h_{0i}	25	26	27	28	29	30	31	32
s_{1i}	Н	Ш	Ю	Щ	Т	Ж	Х	Д
h_{1i}	26	29	32	3	6	9	12	15

Таблица 1. Таблица замены

Использование таблицы замены значительно упрощает процесс шифрования. При шифровании символ исходного текста сравнивается с символами строки soi таблицы. Если произошло совпадение в i-м столбце, то символ исходного текста заменяется символом из строки s1j, находящегося в том же столбце i таблицы.

Расшифрование осуществляется аналогичным образом, но вход в таблицу производится по строке s1i.

Ход выполнения лабораторной работы:

1. Изучить приведенные в методическом описании к лабораторной работе материал и пример шифрования методом простой замены.
2. Получить у преподавателя исходный текст и ключ для шифрования.
3. Выполнить по шагам процедуру шифровании, полученный шифротекст представить в виде блоков информации.
4. Представить результаты преподавателю.
5. Получить у преподавателя шифротекст и ключ для расшифрования.
6. Выполнить по шагам процедуру расшифрования, полученный исходный текст представить преподавателю для проверки.
7. Оформить отчет в установленной форме.
8. Представить результаты работы преподавателю и защитить работу ответами на контрольные вопросы.

Задание:

1. Зашифровать следующий текст: История Тульского государственного университета начинается в 1930 году. Сегодня в инфраструктуру университета входят 18 учебных и 12 лабораторных корпусов, 14 общежитий и ряд других зданий и сооружений, которые компактно расположены в центре Тулы.

- 1

- 2

Русский алфавит		
А ·–	К –·–	Х ····
Б –···	Л ·–··	Ц –·–·
В ·––	М ––	Ч –––·
Г ––·	Н –·	Ш ––––
Д –··	О –––	Щ ––·–
Е ·	П ·––·	Ъ ––·––
Ё ·	Р ·–·	Ы –·––
Ж ···–	С ···	Ь –··–
З ––··	Т –	Э ··–··
И ··	У ··–	Ю ··––
Й ·–––	Ф ··–·	Я ·–·–

Цифры
1 ·————
2 ··–––
3 ···––
4 ····–
5 ·····
6 –····
7 ––···
8 –––··
9 ––––·
0 –––––

2. Придумать свой шифр.

Контрольные вопросы:

1. Определение метода шифрования (шифра)
2. Понятие атаки на шифр (криптоанализа).
3. Понятие криптостойкости и требования, предъявляемые к криптостойкости.
4. Понятие и особенности метода простой замены.
5. Недостатки метода простой замены.

Практическая работа № 8

Тема: «Методы представления знаний: процедурные представления, логические представления, семантические сети, фреймы. Анализ процессов и систем информационной безопасности»

Цель работы научится делать анализ процессов и систем информационной безопасности.

Задания:

1. Описать и сравнить алгоритм нечеткого логического вывода Сугено первого порядка от алгоритма нечеткого логического вывода Сугено нулевого порядка?

2. Описать алгоритм работы нечеткого логического вывода Мамдани для системы информационной безопасности предприятия?

3. Привести основные отличия алгоритма работы нечеткого логического вывода Мамдани от алгоритма работы нечеткого логического вывода Сугено. Указать достоинства и недостатки обоих алгоритмов.

Практическая работа № 9
Тема: ««Анализ параметров безопасности сетей и систем. Нечеткий аппроксиматор. Эффективность нечетких систем управления информационной безопасностью»»

Цель работы научится делать анализ параметров безопасности сетей и систем.

Для построения системы нечеткого вывода используется система MatLab, обладающая достаточно широким функционалом.

Для оценки рисков необходимо задать входные переменные, которыми являются факторы риска: угроза, ущерб и уязвимость.

Выходной переменной является степень риска.

Однако, прежде чем приступать к построению нечеткой модели, необходимо построить функции принадлежностей для каждой из нечетких переменных. Входные переменные имеют значения в интервале от 0 до 1. Чем ближе значение каждой из переменных к единице, тем более высока степень воздействия фактора риска на систему безопасности. Для построения функций принадлежности предлагаем использовать метод построения лингвистических шкал.

Построение нечеткой лингвистической шкалы для каждой из нечетких переменных осуществляется в два этапа:

1) определение множества значений лингвистической переменной xi;

2) размещение значений лингвистической переменной на универсальной шкале от 0 до 1.

На первом этапе речь идет о построении синтаксического правила, порождающего названия значений лингвистической переменной. Процедура выполняется на эвристическом уровне. При этом число термов должно быть не очень большим во избежание затруднений у экспертов при формировании предпочтений при выборе конкретного значения лингвистической переменной. С другой стороны, это число не должно быть слишком малым, чтобы не загрублять чувствительность оценок эксперта.

Далее выбираются названия термов. Должно выполняться требование – однозначное толкование этих названий большинством экспертов.

На втором этапе построения нечеткой лингвистической шкалы задается семантическое правило, сопоставляющее название лингвистической переменной с ее смыслом, т. е. строится функция принадлежности термов множества.

Одним из способов построения функций принадлежности является способ статистического эксперимента. Предположим, что эксперту необходимо оценить в значениях лингвистической переменной «степень угрозы» , угроза принимает значения,

где В – максимально возможная угроза, лежит в интервале [0; В]. Разделим интервал на N отрезков.

Группе экспертов в случайном порядке предъявляются числа из каждого отрезка, интерпретируемые как точечные значения степени угрозы. Эксперт на основе индивидуальных представлений относит предъявленное значение к определенным термам из множества Т. В ходе эксперимента формируется эмпирическая таблица (табл. 1) , каждый элемент которой aij есть суммарное количество отнесения случайного числа из отрезка j к i-му терму.

Таблица 1 Результаты статистического эксперимента

Значение лингвистической переменной «степень угрозы»	Интервал					
Низкий	a11	a12	…	a1 j	…	a1N
Средний	a21	a22	…	a2 j	…	a2N
Высокий	a31	a32	…	a3 j	…	a3N

Очевидно, что если в каждый интервал попадает одинаковые число экспериментов, то степень принадлежности некоторого значения может быть вычислена как отношение числа экспериментов, в котором оно встречалось в определенном интервале шкалы, к максимальному для этого значения числу экспериментов по всем интервалам. Однако на практике это условие может и не соблюдаться (например, эксперт затрудняется отнести оцениваемое значение к какому-либо интервалу). Заметим, что естественными свойствами функции принадлежности являются наличие одного максимума и гладкие, затухающие до нуля фронты. Поэтому до обработки из эмпирической таблицы должны быть удалены явно ошибочные данные. Критерием удаления служит наличие нескольких нулей встроке вокруг этого элемента. Тогда значение функции принадлежности по эмпирической матрице может быть рассчитано по следующему алгоритму.

Цель создания нечеткой модели управления информационной безопасностью заключается в том, чтобы на основе текущего состояния объекта защиты определить значения управляющих переменных, реализация которых обеспечит необходимый уровень защиты.

В классической теории управления базовая модель основана на представлении объекта и процесса в виде некоторых систем.

Объект управления характеризуется конечным множеством входных и выходных переменных. Входные переменные формируются с помощью конечного множества датчиков. На выходе системы управления формируется множество выходных (управляющих) переменных. Значения управляющих перемен-

ных поступают на вход объекта управления и формируют адекватное управляющее воздействие.

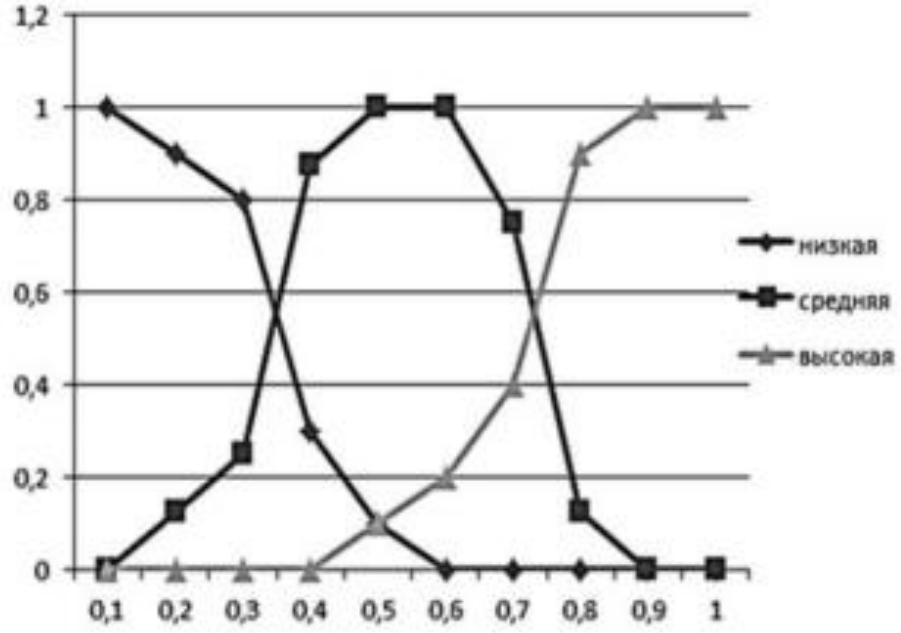


Рис. 1. График функций принадлежности переменной «степень угрозы»

В случае если строится модель нечеткого управления, то классическая система управления заменяется системой нечеткого управления. В качестве данной системы используется система нечеткого вывода с реализацией всех необходимых этапов (рис. 1). Процесс нечеткого вывода представить на основе одного из алгоритмов нечеткого вывода (рис 2).

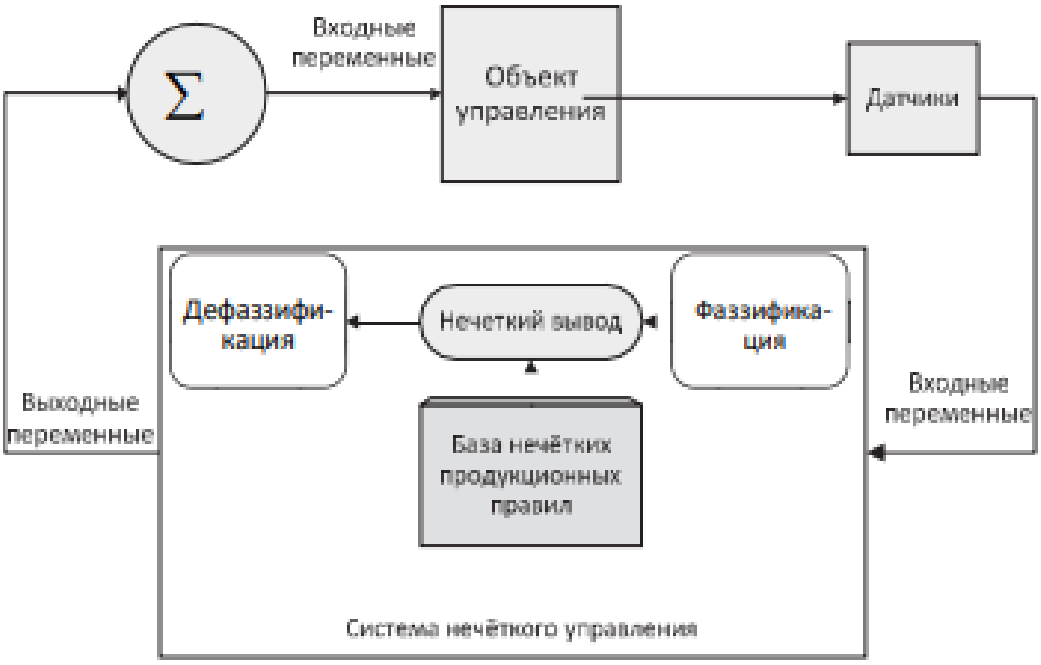


Рис. 2. Схема процесса нечеткого управления

Практическая работа № 10
Тема: ««Моделирование интеллектуальной системы информационной безопасности»»

Цель работы научится выполнять моделирование интеллектуальной системы информационной безопасности.

Задания:

1. Зарегистрировать учётную запись для подключения к облачной платформе
2. Выделить вычислительные ресурсы
3. Разработать модельное предложение БД для размещения на платформе
4. Доставить приложение на платформу

Практическая работа № 11
Защита документов, созданных в Microsoft Word. Защита документов, созданных в Microsoft Excel Защита документов, созданных в Microsoft Access. Защита файла паролем

Цель работы:

Изучение возможностей современных средств защиты документов, созданных в среде приложений OS Microsoft.

Закрепление теоретического материала.

Изучение способов и систем защиты файлов и файловых систем.

Учебно-наглядные пособия и ТСО: ПЭВМ, ОС Windows, пакет Microsoft Office, методическое пособие.

ЗАДАНИЯ:

1. Создать документ в приложении Word офисного пакета Microsoft Office

Используя свойства и возможности приложения Word, защитить созданный файл паролем. Используя настройки атрибутов файла, ограничить доступ к файлу пользователей сети. Используя настройки атрибутов файла, сделать файл «скрытым».

2. Создать документ в приложении Excel офисного пакета Microsoft Office Используя свойства и возможности приложения Excel, защитить созданный файл паролем. Используя настройки атрибутов файла, ограничить доступ к файлу пользователей сети. Используя настройки атрибутов файла, сделать файл «скрытым».

3.1 Создать документ в приложении Access пакета Microsoft Office

Используя свойства и возможности приложения Access, защитить созданный файл паролем. Используя настройки атрибутов файла, ограничить доступ к файлу пользователей сети. Используя настройки атрибутов файла, сделать файл «скрытым»

3.2 Выполнить программу на одном из языков программирования, осуществляющую функцию защиты файла паролем.

Ход выполнения задания: 1. Составить алгоритм 2. Использовать условные операторы 3. Создать необходимые циклы, один из которых использует функцию сравнения пароля 1 цикл на запуск программы используя число ввода пароля до 3 4. Завершение программы неудачей, если число ввода неверного пароля превысило N=3 5. Можете использовать следующие текстовые сообщения (примерные): – «ВВЕДИТЕ ПАРОЛЬ ДЛЯ ВХОДА В ПРОГРАММУ» (Начало выполнения загрузки) – «ПАРОЛЬ НЕВЕРНЫЙ! ИСПОЛЬЗУЙТЕ ЕЩЕ ОДНУ ПОПЫТКУ» (Если пароль введен некорректно) – ДОБРО ПОЖАЛОВАТЬ! (Если пароль введен корректно) – «ВЫ ПРЕВЫСИЛИ ДОПУСТИМОЕ ЧИСЛО ПОПЫТОК! ДО СВИДАНИЯ!» (Если количество неверных попыток ввода пароля превысило допустимое число N=3

Ход выполнения лабораторной работы:

1. Изучить приведенный в методическом описании к лабораторной работе материал.

2. Ответить на контрольные вопросы.

3. Представить отчет по лабораторной работе преподавателю.

Контрольные вопросы:

1. Перечислите свойства файлов (документов), создаваемых в MS Office.

2. В чем заключаются особенности файлов (документов), создаваемых в MS Word?

3. Перечислите порядок установки пароля к созданному файлу в MS Word

4. В чем заключаются особенности файлов (документов), создаваемых в MS Access?

5. Перечислите порядок установки пароля к созданному файлу в MS Access.

6. Назовите назначение основных модулей в блок-схеме алгоритма разработанной Вами программы.

7. При каких условиях в общем случае может быть обеспечен доступ к сетевому ресурсу?

Практическая работа № 12
Защита ПК от вредоносных закладок (разрушающих программных средств)

Цель работы:

Закрепление теоретического материала по изучению действия и защите от вредоносных закладок (разрушающих программных средств).

Изучение способов и правил защиты системы от вредоносных закладок (разрушающих программных средств).

Приборы и оборудование:

Персональный компьютер

ОС MS Windows 7 (MS Windows 10), MS Office, Браузер Microsoft Internet Explorer (Edge)

Теоретические сведения:

К основным разновидностям вредоносного воздействия относятся воздействие на информацию (уничтожение, искажение, модификация) и воздействие на систему (вывод из строя, ложное инициирование действия, модификация содержания выполняемых функций, создание помех в работе). Более детально возможный характер воздействия закладок будет представлен ниже при рассмотрении вопроса об их классификации.

Данный вид защиты для ПК имеет особое значение по ряду причин, а именно:

1) он актуален для всех без исключения пользователей ПК независимо от того, конфиденциальная или открытая информация ими обрабатывается;

2) заражение разрушающими программными средствами (РПС) представляет угрозу повышенной опасности для ПК, чему особенно способствует высокий динамизм обмена информацией как по каналам связи (в сетях ЭВМ), так и посредством гибких дисков;

3) защита ПК от РПС требует особого профессионализма, поскольку многие из них носят специфический индивидуальный характер, а их нейтрализация и устранение сопряжены с программными манипуляциями нередко весьма сложного и даже искусного характера.

Известные в настоящее время закладки осуществляются аппаратным или программным путем.

Аппаратные закладки могут быть осуществлены в процессе изготовления ПК, ее ремонта или проведения профилактических работ. Реальная угроза таких закладок создается массовым и практически неконтролируемым распространением ПК. Особая опасность аппаратных закладок заключается в том, что

они могут длительное время не проявлять своих вредоносных воздействий, а затем начать их осуществление или по истечении определенного времени, или при наступлении некоторого состояния ПК (например, при заполнении данными жесткого магнитного диска до заданного уровня), или по специальной, подаваемой дистанционно команде. Заблаговременное обнаружение аппаратных закладок возможно только в условиях проверок с использованием специальных методов и средств.

Программные закладки (РПС) с точки зрения массового пользователя представляются особо опасными в силу сравнительной (относительно аппаратных) простоты их осуществления, высокой динамичности их распространения и повышенной трудности защиты от них. Так, если в итоге специальных проверок аппаратные закладки не были обнаружены или они были ликвидированы (нейтрализована возможность их действия), то с высокой степенью можно быть уверенными в их отсутствии в соответствующей ПК.

Программные же закладки могут появиться в любое время, чему особенно способствуют следующие обстоятельства:

1) массовый обмен информацией на гибких МД, принявший к настоящему времени характер броуновского движения;

2) широкое распространение копий программ, приобретенных незаконным путем;

3) возможности дистанционного воздействия на ПК, подключенные к сети;

4) широкий и непрерывно растущий диапазон разновидностей закладок, что усложняет процессы их обнаружения и нейтрализации.

В силу изложенных причин защиту от программных закладок рассмотрим несколько детальней, выделив при этом следующие вопросы:

1. Классификация закладок и их характеристики.

2. Принципиальные подходы и общая схема защиты от закладок.

3. Методы и средства защиты.

2. Рекомендации пользователям ПК по защите от программных закладок.

Классификация закладок и их общие характеристики

К сожалению, научно обоснованная классификация закладок до настоящего времени пока не разработана, что объясняется отчасти недостаточным объемом статистических данных, а отчасти тем, что работы по защите от закладок различных разновидностей ведутся изолированно. Системные исследования и разработки еще только предстоит выполнить.

Поэтому излагаемое ниже должно рассматриваться лишь в качестве первого приближения.

Всякая классификация осуществляется по вполне определенному и существенно значимому критерию или по их совокупности. Исходя из целей защиты от вредоносного воздействия закладок, их целесообразно классифицировать по следующей совокупности критериев:

1) характеру вредоносного воздействия на АСОД;

2) способу реализации;

3) способу проникновения в АСОД;

4) способность к саморазмножению.

Основные значения первого критерия могут быть представлены в следующем виде:

1) уничтожение или искажение программ и/или массивов данных;

2) формирование каналов несанкционированного получения информации;

3) вывод АСОД из числа действующих, т. е. приведение ее в такое состояние, при котором она не может осуществлять свои основные функции;

4) инициирование выполнения предусмотренных в АСОД функций (например, ложная подача команды на остановку производства в автоматизированных системах управления технологическими процессами);

5) создание препятствий в выполнении функций АСОД (например, блокировка отображения информации на экране дисплея, выдачи на печать и др.).

Возможные значения второго критерия (способ реализации) могут быть представлены следующим перечнем:

1) аппаратный;

2) программный;

3) организационный.

Первые два способа реализации рассмотрены выше, они, вообще говоря, являются основными. Однако в общем случае можно предположить возможность создания также организационных закладок. Например, в инструкции об уничтожении информации, находящейся в ЭВМ, в злоумышленных целях можно предусмотреть преждевременное ее уничтожение или, наоборот, сохранение той информации, которую надлежало бы уничтожить. В инструкции по использованию криптографических средств злоумышленно можно внести такие положения, выполнение которых может дать крипто-аналитику дополнительную информацию, облегчающую криптоанализ шифртекста. Нетрудно предположить возможность создания ряда других организационных закладок.

По способу проникновения в АСОД (третий критерий классификации) закладки могут быть разделены на следующие группы:

1) злоумышленно создаваемые в процессе производства аппаратуры ЭВТ и компонентов ее программного обеспечения;

2) бессознательно вносимые персоналом или пользователями АСОД в процессе ее функционирования;

3) злоумышленно вносимые в процессе функционирования АСОД;

4) злоумышленно создаваемые в процессе ремонта аппаратуры или модификации АСОД.

Наконец, по способности к размножению (четвертый критерий классификации) закладки естественным образом делятся на две разновидности:

1) саморазмножающиеся;

2) несаморазмножающиеся.

К настоящему времени известно значительное количество закладок, получивших такие условные наименования: троянский конь, бомба, ловушка, люк, вирус, червь.

Отличительные особенности данных разновидностей могут быть охарактеризованы следующим образом.

Троянский конь — несаморазмножающееся РПС, способное осуществлять несанкционированное считывание данных, их уничтожение и другие деструктивные функции.

Бомба — несаморазмножающееся РПС одноразового использования, приводящееся в действие в определенных условиях (в заданное время, в заданном состоянии ЭВМ, по команде извне) и осуществляющее крупномасштабное уничтожение информации.

Ловушка — несаморазмножающаяся программа, осуществляющая несанкционированный перехват информации и запись ее в соответствующее поле ЗУ или выдачу в канал связи.

Люк — несаморазмножающаяся программа, обеспечивающая злоумышленнику возможности несанкционированного доступа к защищаемой информации.

Вирус — саморазмножающееся РПС, способное уничтожать или изменять данные и/или программы, находящиеся в ЭВМ.

Червь — саморазмножающееся РПС, способное уничтожать элементы данных или программ.

Принципиальные подходы и общая схема защиты от закладок. Основу защиты составляют следующие функции:

1) создание таких условий, при которых дестабилизирующие факторы (ДФ) не могут появляться;

2) предупреждение появления ДФ, даже если для этого имеются условия;

3) обнаружение появления ДФ;

4) предупреждение воздействия на информацию появившихся ДФ;

5) обнаружение негативного воздействия ДФ на информацию;

6) локализация негативного воздействия ДФ на информацию;

7) ликвидация последствий воздействия ДФ.

Методы и средства защиты. Для защиты от закладок должны использоваться методы анализа, синтеза и управления, организационно-правовые, аппаратные и программные средства. Ниже приводятся общие сведения о средствах, специфических для защиты от закладок.

Средства борьбы с вирусами и другими вредоносными закладками можно разделить на юридические, организационно-административные, аппаратные и программные.

Юридические средства сводятся к установлению ответственности за умышленное создание и распространение вирусов и других закладок в целях нанесения ущерба, хотя доказать авторство и умышленность создания таких программ довольно трудно.

Следует признать, что на Западе соответствующие правовые нормы разработаны гораздо лучше, чем в России. Назовем некоторые законы, применяемые в западных странах для борьбы с компьютерными преступлениями:

1) Закон о поддельных средствах доступа, компьютерном мошенничестве и злоупотреблении (США).

2) Федеральный закон о частной тайне (США).

3) Закон о предупреждении экономических преступлений (Германия).

4) Закон об авторском праве (Германия).

5) Федеральный закон о защите данных (Германия).

6) Закон об авторском праве и поправки к нему (Великобритания).

7) Закон о защите данных (Великобритания).

8) Закон об обработке данных, о файлах данных и личных свободах (Франция).

В ряде стран введены соответствующие статьи в уголовные кодексы.

Перечисленные законы позволяют вести достаточно эффективную борьбу с изготовителями вредоносных программ. Например, еще в начале 1989 года американский студент был приговорен судом к трем месяцам тюремного заключения и штрафу в 270 тысяч долларов за разработку вируса, которым были выведены из строя шесть тысяч компьютеров Министерства обороны США.

В Российской Федерации в последнее время также предпринимаются серьезные усилия по созданию юридической основы борьбы с рассматриваемыми угрозами. Так, в принятый недавно Уголовный кодекс Российской Федерации введено три статьи (272-274), по которым предусмотрена ответственность за компьютерные преступления, причем самое строгое наказание (от 3 до 7 лет тюремного заключения) предписывается статьей 273 — за создание, использование и распространение вредоносных программ.

Организационно-административная защита от вредоносных программ заключается в выработке и неукоснительном осуществлении организационных и организационно-технических мероприятий, направленных на предупреждение заражения компьютеров этими программами, обнаружение заражения, нейтрализацию негативного их воздействия и ликвидацию последствий. Названные мероприятия должны осуществляться как в организациях — разработчиках программных средств, так и в организациях, эксплуатирующих эти программы.

В организациях-разработчиках весьма целесообразно из состава высококвалифицированных программистов создавать специальные группы для выполнения следующих функций:

1) определения потенциально возможных источников вредоносных программ и выработка рекомендаций по их обходу;

2) выявления и изучения всех нештатных ситуаций, возникающих при разработке программного обеспечения, документального оформления результатов анализа и оповещение всех заинтересованных при выявлении опасностей;

3) регулярного контроля состояния программного обеспечения и средств борьбы с вредоносными программами;

4) возможно более быстрой ликвидации последствий произошедшей атаки вредоносных программ и изготовления соответствующих средств защиты;

5) оказания методической помощи своим абонентам в организации необходимой защиты от вредоносных программ.

Основными мероприятиями по защите программ и данных в организациях, использующих программы, представляются следующие:

1) приобретение только законным путем необходимых технических средств и программ, сертифицированных на отсутствие вредоносных закладок;

2) создание эталонных копий основных программ и резервирование баз данных;

3) организация автоматизированной обработки данных с соблюдением всех приемов и правил;

4) периодическая тщательная проверка состояния программного обеспечения и баз данных;

5) проверка психологических особенностей сотрудников при приеме на работу;

6) создание и поддержание в коллективах здорового морально-психологического климата.

Из аппаратных средств защиты рекомендуются следующие:

1) форматирование диска (для винчестера — полное стирание и переразметка), перезагрузка операционной системы и восстановление программ с незараженных копий;

2) заклеивание (закрывание) отверстия защиты записи дискеты;

3) физическая блокировка ключом клавиатуры ЭВМ;

4) запрет и регистрация попыток записи в файлы операционной системы в области памяти, занятые системной информацией.

Известны и другие, подобные перечисленным, меры: разделение областей памяти между программами, разделение программ по приоритетам и т. п.

В целях повышения эффективности защиты ЭВМ от вредоносных программ в последнее время ведутся разработки защищенных противовирусных компьютеров и специальных плат, встраиваемых в существующие компьютеры.

Важнейшим компонентом среди средств защиты от вредоносных программ выступают специальные программы, получившие на звание антивирусных. Известные к настоящему времени антивирусные программы по функциональному признаку делятся на 4 класса:

— класс А — предупреждение заражения;

— класс Б — выявление последствий заражения;

— класс В — минимизация причиненного ущерба;

— класс Г — общего характера.

Программы класса А делятся на 5 групп следующего назначения:

А1 — фильтры, следящие за операциями других исполняемых программ и реагирующие на подозрительные действия;

А2 — резидентные детекторы и фаги, следящие за появлением в оперативной памяти конкретных вирусов и подающие при их появлении специальные сигналы оператору;

А3 — иммунизаторы, изменяющие файлы и области оперативной памяти таким образом, что вирус их после этого не заражает;

А4 — разграничители доступа, ограничивающие распространение вирусов путем разграничения доступа к ресурсам ЭВМ, программам и массивам данных со стороны других программ и пользователей;

А5 — преобразователи параметров операционной среды, реализующие изменение соглашений, принятых в операционной системе (форматы записей, команды, расположение системной информации и др.), недоступные разработчикам вирусов и тем самым препятствующие заражению ЭВМ.

Программы класса Б делятся на 6 групп следующего функционального назначения:

Б1 — нерезидентные детекторы и фаги, осуществляющие просмотр запоминающих устройств, определяющие зараженность файлов и дисков и организующие их лечение;

Б2 — программы проверки подозрительных характеристик, осуществляющие просмотр запоминающих устройств и выявление таких характеристик,

которые могут говорить о наличии вируса в системе. К таким характеристикам относятся недопустимые значения отдельных полей в заголовке файла, подозрительные переходы, странные изменения в программах и т. п.;

Б3 — программы, осуществляющие просмотр файлов и носителей, определение различных их характеристик (контрольные суммы, криптографические суммы, длины, даты и времени создания и др.) и сравнение этих величин с эталонами в целях определения возможного заражения;

Б4 — программы, осуществляющие слежение и регистрацию в системном журнале операций, осуществляемых на ЭВМ. При заражении анализ журнала помогает выявить источник заражения, характер поведения вируса;

Б5 — программы-ловушки (дрозофилы, уловители), специально выделяемые для заражения, которые, заражаясь, сигнализируют о наличии вируса;

Б6 — программы автономной защиты файла, защищающие файлы от вирусов путем дописывания своей копии к защищаемым модулям.

Программы класса В (минимизирующие ущерб, причиненный заражением РПС) делятся на следующие 3 группы:

В1 — программы полного копирования, предназначенные для создания резервных копий программного обеспечения;

В2 — программы частичного копирования, предназначенные для копирования и восстановления наиболее уязвимых частей диска (Boot-сектор, FAT, корневое оглавление);

В3 — программы, прерывающие вычислительный процесс, т. е. осуществляющие принудительное прерывание вычислительного процесса в целях локализации распространения вируса.

Программы класса Г (общего назначения) предназначены не для прямой борьбы с вирусами, а для оказания помощи в этой борьбе. Эти программы делятся на 5 групп следующего назначения:

Г1 — программы просмотра диска, позволяющие отображать значения каждого сектора, копировать одну физическую область в другую. Применяются для определения целостности отдельных частей диска, наличия вируса в файлах и внесения небольших изменений;

Г2 — программы, позволяющие искать на диске контекст определенного содержания.

С их помощью можно найти участки кодов вирусов и пораженные ими сектора;

ГЗ — программы, позволяющие восстанавливать отдельные части диска;

Г4 —. программы, реализующие просмотр состояния оперативной памяти, состав и характеристики находящихся там модулей;

Г5 — программы, позволяющие упорядочить информацию на диске на физическом уровне по заранее заданному закону.

Контрольные вопросы:

1. Перечислите уровни защиты компьютерных и информационных ресурсов.

2. Дайте понятие вредоносных закладок (разрушающих программных средств), перечислите разновидности и особенности.

3. Какие действия в рамках защитных мероприятий требуется выполнять для защиты от РПС?

Литература

Васильков А.В. Безопасность и управление доступом в информационных системах / А.В. Васильков, И.А. Васильков.— Москва : ФОРУМ: ИНФРА-М, 2013.— 368 с.

2. Жигулин Г.П. Организационное и правовое обеспечение информационной безопасности / Г.П. Жигулин.— Санкт-Петербург : СПбНИУИТМО, 2014.— 173 с.

3. Теоретические основы компьютерной безопасности / П.Н. Девянин [и др.].— Москва : Радио и связь, 2000.— 192 с.

4. Бардаев Э.А. Документоведение : учебник для студ. высш. учеб. заведений / Э.А. Бардаев, В.Б. Кравченко.— Москва : Издательский центр «Академия», 2008.— 304 с.

5. Малюк А.А. Введение в защиту информации в автома тизированных системах / А.А. Малюк, С.В. Пазизин, Н.С. Погожин.— Москва : Горячая линия — Телеком, 2001.— 148 с.

6. Мельников В.В. Безопасность информации в автоматизированных системах / В.В. Мельников.— Москва : Финансы и статистика, 2003.— 368 с.

7. Гайдамакин Н.А. Разграничение доступа к информации в компьютерных системах / Н.А. Гайдамакин.— Екатеринбург : Изд-во Урал. ун-та, 2003.— 328 с.

8. Зегжда Д. П. Основы безопасности информационных систем / Д.П. Зегжда, А.М. Ивашко.— Москва : Горячая линяя — Телеком, 2000.— 452 с.

9. Барсуков В.С. Безопасность: технологии, средства, услуги/ В.С.Барсуков.— Москва : КУДИЦ-ОБРАЗ, 2001–496с.

10. Расторгуев С.П. Информационные войны / С.П. Расторгуев. — Москва : «Финансы и статистика», 1998.— 415 с

11. Хорев, П.Б. Методы и средства защиты информации в компьютерных системах : учеб.пособие для вузов / П.Б.Хорев .— 2-е изд.,стер. — М. : Академия, 2006 .— 256с. : ил. — (Высшее профессиональное образование:Информатика и вычислительная техника) .— Библиогр.в конце кн. — ISBN 978-5-7695-3288-2 /в пер./ : 180.40 (6 экз.).

12. Куприянов, А.И. Основы защиты информации : учеб.пособие / А.И.Куприянов,А.В.Сахаров,В.А.Шевцов .— 2-е изд.,стер. — М. : Академия, 2007 .— 256с. : ил. — (Высшее профессиональное образование:Радиоэлектроника) .— Библиогр.в конце кн. — ISBN 978-5-7695-4416-3 /в пер./ : 247.00 (10 экз.)

13. Мельников, В.П. Информационная безопасность и защита информации : учеб.пособие для вузов / В.П.Мельников,С.А.Клейменов,А.М.Петраков;под ред.С.А.Клейменова .— 3-е изд.,стер. — М. : Академия, 2008 .— 336с. — (Высшее профессиональное образование:Информатика и вычислительная техника) .— Библиогр.в конце кн. — ISBN 978-5-7695-4884-0 /в пер./ : 239.80 (5 экз.).

14. Остапенко, Г.А. Информационные операции и атаки в социотехнических системах : учеб.пособие для вузов / Г.А.Остапенко;под ред.В.И.Борисова .— М. : Горячая линия-Телеком, 2007 .— 134с. : ил. — (Учебное пособие для высших учебных заведений.Специальность) .— Библиогр.в конце кн. — ISBN 5-93517-288-7 : 102.85 (3 экз.).