МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ВОЛГОГРАДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

На правах рукописи

Д.В. Быков

Защита информации

Учебное пособие

Волгоград
2021

УДК 004.056

Быков Д.В.
Защита информации : учеб. пособие / Д.В. Быков; ВолгГТУ. – Волгоград, 2021. – 39 с.

В учебном пособии рассмотрены вопросы, связанные с обеспечением защиты информации в системах искусственного интеллекта.

Учебное пособие предназначено для магистров, обучающихся по программам магистратуры по профилю «искусственный интеллект» по направлениям 09.04.01 «Информатика и вычислительная техника», 09.04.03 «Прикладная информатика», 09.04.02 «Информационные системы и технологии». Учебное пособие выполнено в рамках реализации гранта на разработку программ бакалавриата и программ магистратуры по профилю «Искусственный интеллект», а также на повышение квалификации педагогических работников образовательных организаций высшего образования в сфере искусственного интеллекта (конкурс 2021-ИИ-01 от 10.06.2021).

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Защита информация является одной из важнейших задач при построении и эксплуатации систем искусственного интеллекта. В данном курсе рассматриваются как общие вопросы реализации мер подобной защиты информации.

1. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ К ПРАКТИЧЕСКИМ ЗАНЯТИЯМ

1.1. Практика №1. Информационная безопасность (ИБ) в области искусственного интеллекта. Основные понятия.

1.1.1. Цель практической работы

Цель практической работы №1 состоит в том, чтобы ввести в курс задач, решаемых при обеспечении ИБ в области искусственного интеллекта.

1.1.2. 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

1.2. Практика №2. Основные стандарты в области обеспечения информационной безопасности систем искусственного интеллекта. Политика безопасности

1.2.1. Цель практической работы

Цель практической работы №2 состоит в изучении основных стандартов информационной безопасности систем искусственного интеллекта.

1.2.2. Описание практической работы

Рассматриваются практические примеры применения стандартов информационной безопасности систем искусственного интеллекта на основании 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 логически с 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 меры. 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 компании
- 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.

1.3. Практика №3. Основные виды сетевых и компьютерных угроз. Средства и методы защиты от сетевых компьютерных угроз

1.3.1. Цель практической работы

Цель практической работы №3 состоит в рассмотрении основных видов сетевых и компьютерных угроз и методов их нейтрализации.

1.3.2. Описание практической работы

Рассматриваются на практике основные виды сетевых и компьютерных угроз:

1. Анализ сетевого трафика

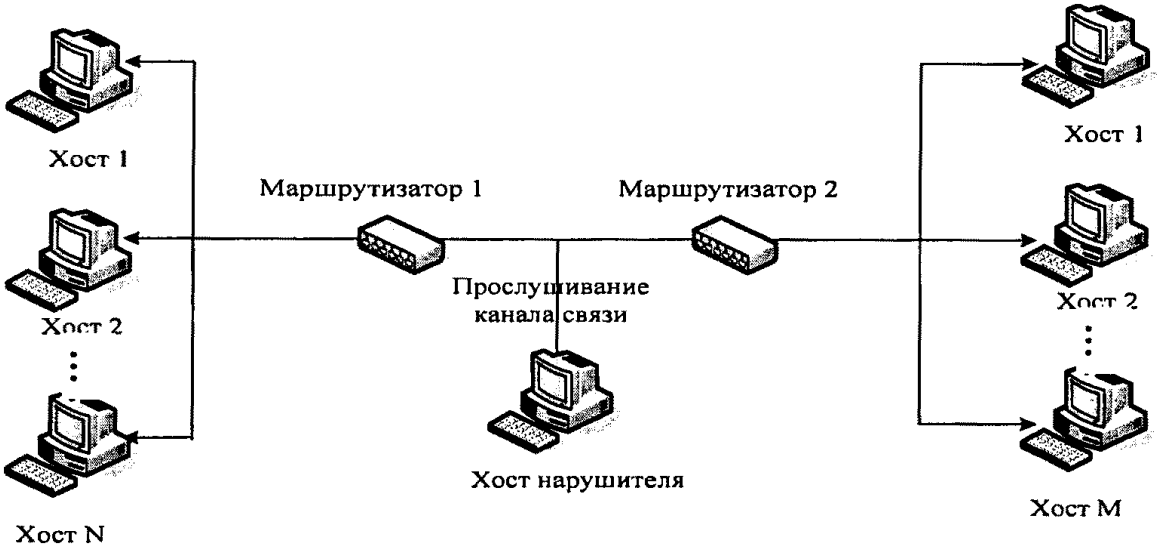

Схема реализации угрозы "Анализ сетевого трафика"

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 ходе реализации 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 идентификаторами абонентов 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.

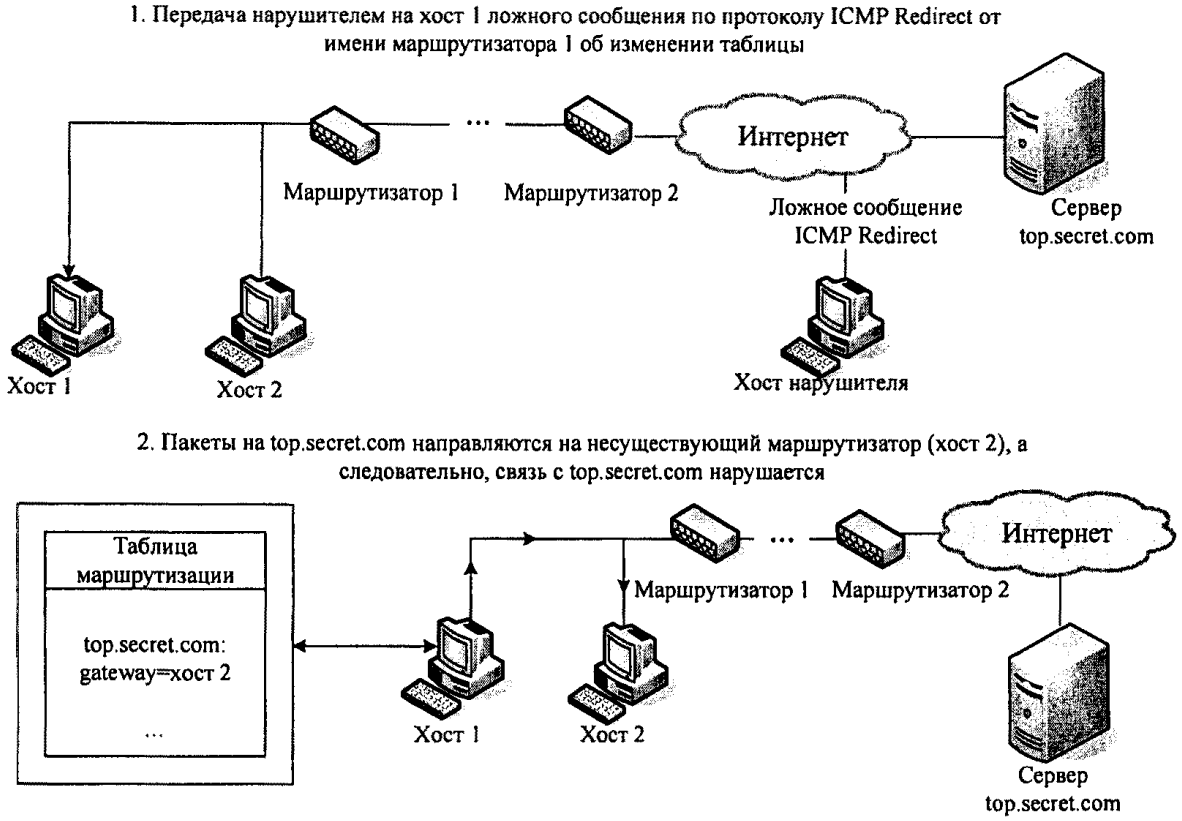

Схема реализации атаки "Навязывание ложного маршрута" (внутрисегментное) с использованием протокола ICMP с целью нарушения связи

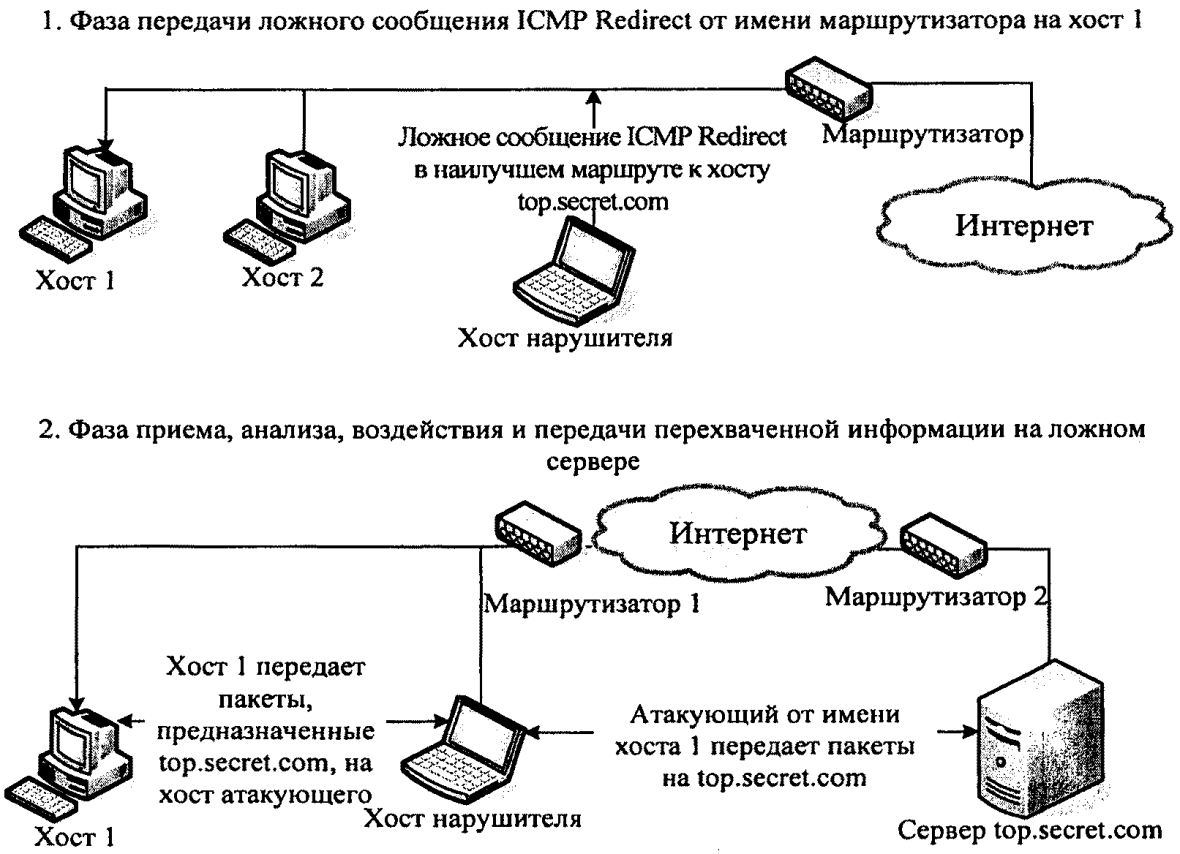

Схема реализации угрозы "Навязывание ложного маршрута" (межсегментное) с целью перехвата трафика

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 проходить через ложный объект сети.

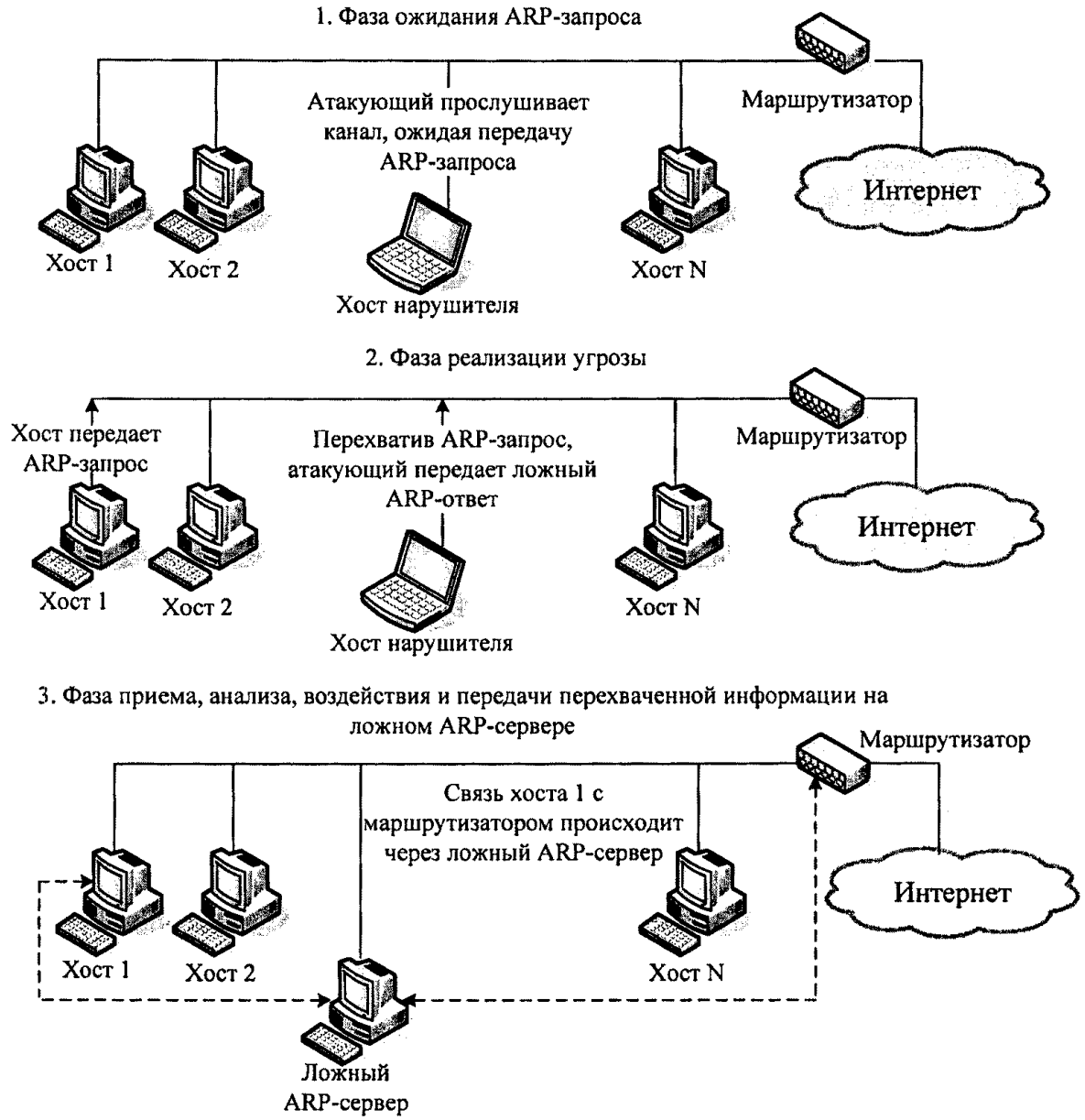

Схема реализации угрозы "Внедрение ложного ARP-сервера"

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 эхо-запросов 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, доступности информации 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 на активизации 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, вызванного 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 типа Back 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 запущена клиент-программа, и обмен с ней сообщениями о готовности;
- передача перехваченной информации клиенту или предоставление ему контроля над атакуемым компьютером.

2. Методические указания к лабораторным работам

2.1 Лабораторная работа № 1. Методы анализа рисков. Понятие уязвимости. Классификация угроз. Методы оценки ущерба от реализации угроз информационной безопасности систем искусственного интеллекта.

2.1.1 Цели и задачи

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

Задачи:

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

2.1.2 Теоретические положения

Теоретические положения отражены в нормативной документации ФСТЭК России.

2.1.3 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.

2.1.4. Варианты заданий

Выполнить этапы анализа уязвимостей на виртуальных машинах со следующими ОС:

1. Windows 10

2. Windows 8.1

3. Windows 7

4. Windows Server 2012.

5. Windows Server 2016.

2.1.5 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 на флэш-накопитель и продублировать на электронную почту).

2.1.6 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.

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

2.2 Лабораторная работа № 2. Специализированные программно-аппаратные средства защиты информации для систем искусственного интеллекта. Основные направления применения криптографических технологий при защите систем искусственного интеллекта

2.2.1 Цели и задачи

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.

2.2.2 Теоретические положения

Теоретические положения отражены в нормативной документации ФСТЭК России.

2.2.3 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 комплекса технических средств.
4. Выбор СКЗИ для решения задачи обеспечения ИБ.

2.2.4. 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.

2.2.5 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 на флэш-накопитель и продублировать на электронную почту).

2.2.6 Вопросы и задания

1. Повторить и закрепить принципы формулирования требований к мерам защиты.

2. Повторить и закрепить требования к применению СКЗИ.

2.3 Лабораторная работа № 3. Принципы организации и примеры систем обнаружения вторжений, мониторинга защищенности локальной и сетевой компьютерной среды

2.3.1 Цели и задачи

Целью работы является ознакомление с особенностями обнаружения вторжений и организации системы мониторинга.

Задачи:

1. Рассмотреть принципы работы систем обнаружения вторжений.

2. Рассмотреть принципы применения систем мониторинга.

2.3.2 Теоретические положения

Теоретические положения отражены в нормативной документации ФСТЭК России.

2.3.3 Порядок выполнения работы

1. Рассмотрение вариантов построения систем обнаружения вторжений.
2. Рассмотрение наиболее популярных систем обнаружения вторжений.
3. Рассмотрение принципов работы систем мониторинга.
4. Тестовый запуск системы мониторинга инфраструктуры.

2.3.4. Варианты заданий

В качестве индивидуального варианта студенты рассматривают анализ применения систем обнаружения вторжений и систем мониторинга для выполнения требований:

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.

2.3.5 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 на флэш-накопитель и продублировать на электронную почту).

2.3.6 Вопросы и задания

1. Повторить и закрепить информацию из Приказа № 17 от 13.02.2013 ФСТЭК России.

2. Повторить и закрепить информацию из Приказа № 21 от 18.02.2013 ФСТЭК России.

3. Повторить и закрепить информацию из документации по обеспечению безопасности АС.

4. Повторить и закрепить информацию из документации по обеспечению безопасности КИИ.

3. МЕТОДИЧЕСКИЕ УКАЗАНИЯ К ВЫПОЛНЕНИЮ КОНТРОЛЬНОЙ РАБОТЫ

3.1. Задание на контрольную работу и методические указания по ее выполнению

На контрольную работу студенту выдается индивидуальное задание (по вариантам), заключающееся в разработке документа «Модель угроз и нарушителя безопасности».

Работа выполняется параллельно и в контексте индивидуальных заданий к лабораторному практикуму по дисциплине. Оформляется в письменной форме в течение 10 недель с момента выдачи задания. Контрольный срок сдачи – последний месяц семестра.

Правила оформления контрольной работы

- контрольная работа оформляется в редакторе MS Word / OpenOffice (*.doc, *.docx, *.odt);
- листы формата А4, ориентация книжная;
- поля: левое – 2 см, остальные – по 1 см;
- шрифт – Times New Roman;
- размер шрифта 14 pt;
- междустрочный интервал – 1,5;
- абзацный отступ – 1,25 см;
- нумерация страниц сквозная, номер на первой странице не ставится;
- в конце работы необходим список использованной литературы согласно ГОСТ Р 7.0.5 – 2008;
- объем работы зависит от степени раскрытия основных пунктов контрольной работы.

3.2. Примерное содержание контрольной работы

Примерное содержание контрольной работы

1. Титульный лист.

2. Формулировка варианта задания.

3. Основная часть, включающая:

1) Описание объекта защиты, для которого производится моделирование угроз.

2) Определение негативных последствий от реализации (возникновения) угроз безопасности информации.

3) Определение возможных объектов воздействия угроз безопасности информации.

4) Определение источников угроз безопасности информации.

5) Оценка способов реализации (возникновения) угроз безопасности информации.

6) Оценка актуальности угроз безопасности информации.

3.3. Примерные варианты заданий контрольной работы

Примерный список вариантов контрольной работы:

1. Разработка модели угроз и нарушителя для системы фильтрации электронной почты

2. Разработка модели угроз и нарушителя для системы чат-бота

3. Разработка модели угроз и нарушителя для системы голосового помощника

4. Разработка модели угроз и нарушителя для поисковой системы.

ЗАКЛЮЧЕНИЕ

В рамках курса на практических примерах и в лабораторном практикуме рассматриваются общие вопросы реализации мер защиты информации в области искусственного интеллекта.

РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА ПО КУРСУ

1. Нестеров, С. А. Основы информационной безопасности : учебник для вузов / С. А. Нестеров. — Санкт-Петербург : Лань, 2021. — 324 с. — ISBN 978-5-8114-6738-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/165837 (дата обращения: 14.10.2021).

2. Защита информации в центрах обработки данных : учебное пособие / И. А. Ушаков, В. А. Десницкий, А. А. Чечулин [и др.]. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2019. — 92 с. — Текст : электронный // Лань : электронно-библиотечная система. — Режим доступа: https://e.lanbook.com/book/180085 (дата обращения: 10.10.2021).

3. Лукша, М. Kubernetes в действии / М. Лукша ; перевод с английского А. В. Логунов. — Москва : ДМК Пресс, 2019. — 672 с. — ISBN 978-5-97060-657-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/131688 (дата обращения: 14.10.2021).

4. Журавлев, А. Е. Инфокоммуникационные системы. Аппаратное обеспечение : учебник для вузов / А. Е. Журавлев, А. В. Макшанов, А. В. Иванищев. — 2-е изд., стер. — Санкт-Петербург : Лань, 2021. — 392 с. — ISBN 978-5-8114-8514-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/176657 (дата обращения: 14.10.2021). — Режим доступа: для авториз. пользователей.

Учебное издание

Дмитрий Владимирович Быков

ЗАЩИТА ИНФОРМАЦИИ

Учебное пособие

Волгоградский государственный технический университет.
400005, г. Волгоград, просп. В. И. Ленина, 28, корп. 1.