МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ВОЛГОГРАДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

На правах рукописи

Д.В. Быков

Безопасность систем искусственного интеллекта

Учебное пособие

Волгоград
2021

УДК 004.056:004.8

Быков Д.В.

Безопасность систем искусственного интеллекта : учеб. пособие / Д.В. Быков; ВолгГТУ. – Волгоград, 2021. – 35 с.

В учебном пособии рассмотрены вопросы, связанные с обеспечением безопасности систем искусственного интеллекта.

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

Обеспечение безопасности информация является одной из важнейших задач при построении и эксплуатации систем искусственного интеллекта. В данном курсе рассматриваются как общие вопросы реализации мер обеспечения ИБ.

1. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ К ПРАКТИЧЕСКИМ ЗАНЯТИЯМ

1.1. Практика №1. Методологические основы комплексной системы защиты информации систем искусственного интеллекта. Определение состава защищаемой информации.

1.1.1. Цель практической работы

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

1.1.2. Описание практической работы

Рассматриваются основные понятия и составляющие процесса обеспечения информационной безопасности в системах искусственного интеллекта.

Пример задач:

1. Изучить состав основных этапов обеспечения информационной безопасности, включая:
    a. Предпроектное обследование / аудит информационной безопасности.
    b. Моделирование угроз информационной безопасности и составление модели нарушителя.
    c. Классификация систем искусственного интеллекта.
    d. Формализация требований к системе защиты систем искусственного интеллекта в виде технического (частного технического) задания на систему защиты.
    e. Разработка технических решений в соответствии с актуальными угрозами информационной безопасности и требованиями технического задания.

f. Оформление комплекта организационно-распорядительной документации.
g. Внедрение средств защиты информации.
h. Проведение предварительных испытаний, опытной эксплуатации, приемочных испытаний системы защиты.
i. Проведение аттестационных испытаний.

2. Рассмотреть состав мероприятий при проведении предпроектного обследования:
    a. описание информационно-телекоммуникационной инфраструктуры, используемой для работы информационной системы искусственного интеллекта;
    b. определение состава и характеристик программно-аппаратного комплекса автоматизированных рабочих мест и серверов, участвующих в работе системы искусственного интеллекта;
    c. определение характеристик системы искусственного интеллекта.
3. Рассмотреть состав мероприятий при проведении моделирования угроз информационной безопасности и составление модели нарушителя:
    a. классификация угроз информационной безопасности;
    b. классификация нарушителей по требованиям ФСТЭК России;
    c. классификация уязвимостей ИС;
    d. проведение комплексного анализа нетиповых уязвимостей в дополнение к рекомендациям ФСТЭК России и ФСБ России;
    e. оценка исходного уровня защищенности, вероятности реализации угрозы, опасности угрозы, определение актуальности угрозы для каждой ИС;
    f. оценка модели нарушителя по методикам ФСБ России и ФСТЭК России.

4. Рассмотреть состав мероприятий при классификации систем искусственного интеллекта.
5. Рассмотреть состав мероприятий при формализации требований к системе защиты систем искусственного интеллекта в виде технического (частного технического) задания на систему защиты.
6. Рассмотреть состав мероприятий при разработке технических решений в соответствии с актуальными угрозами информационной безопасности и требованиями технического задания:
    a. разработка пояснительной записки;
    b. разработка схемы структурная комплекса технических средств;
    c. разработка схемы функциональной структуры системы защиты информации;
    d. разработка спецификации поставки.
7. Рассмотреть состав мероприятий при оформлении комплекта организационно-распорядительной документации, в рамках которого:
    a. назначаются ответственные за организацию обработки информации;
    b. назначаются ответственные за обеспечение безопасности системы искусственного интеллекта;
    c. утверждаются перечень систем искусственного интеллекта и сведений, обрабатываемых в них;
    d. утверждаются список лиц, получивших доступ к системе искусственного интеллекта;
    e. утверждается контролируемая зона;
    f. определяется мероприятия по контролю доступа к системам искусственного интеллекта;
    g. утверждаются инструкции по обработке данных в системе искусственного интеллекта;

h. утверждаются инструкции по обработке информации с использованием средств криптографических средств защиты информации;
i. утверждаются правила доступа к машинным носителям информации;
j. определяются мероприятия по контролю состояния защищенности системы искусственного интеллекта.

8. Рассмотреть состав мероприятий при внедрении средств защиты информации.
9. Рассмотреть состав мероприятий при проведении предварительных испытаний, опытной эксплуатации, приемочных испытаний системы защиты, в рамках которых:
    a. разрабатывается программа предварительных испытаний системы защиты;
    b. проводятся предварительные испытания системы защиты;
    c. подготавливается протокол проведения предварительных испытаний системы защиты;
    d. разрабатывается программа опытной эксплуатации системы защиты;
    e. проводится опытная эксплуатация системы защиты;
    f. подготавливается отчет опытной эксплуатации системы защиты и акт допуска к приёмочным испытаниям;
    g. проводятся приёмочные испытания системы защиты;
    h. подготавливается протокол проведения приемочных испытаний системы защиты и акт передачи системы в постоянную эксплуатацию.
10. Рассмотреть состав мероприятий при проведении аттестационных испытаний, в рамках которых:

a. проводятся аттестационные испытания в соответствии с ранее разработанной программой и методикой;
b. разрабатывается заключение по итогам аттестационных испытаний и аттестат соответствия.

1.2. Практика №2. Источники, способы и результаты дестабилизирующего воздействия на информацию. Каналы и методы несанкционированного доступа к информации.

1.2.1. Цель практической работы

Цель практической работы №2 состоит в изучении основных Источников способов и результатов дестабилизирующего воздействия на информацию.

1.2.2. Описание практической работы

Рассмотрим источники дестабилизирующего воздействия на информацию. К ним относятся:

1. Люди;
2. Технические средства отображения (фиксации), хранения, обработки, воспроизведения, передачи информации, средства связи;
3. Системы обеспечения функционирования технических средств отображения, хранения, обработки, воспроизведения и передачи информации;
4. Технологические процессы отдельных категорий промышленных объектов;
5. Природные явления.

Самым распространенным, многообразным и опасным источником дестабилизирующего воздействия на защищаемую информацию являются люди, которые делятся на следующие категории:

— сотрудники данного предприятия;

— лица, не работающие на предприятии, но имеющие доступ к защищаемой информации предприятия в силу служебного положения (из вышестоящих, смежных (в том числе посреднических) предприятий, контролирующих органов государственной и муниципальной власти и др.);

— сотрудники государственных органов разведки других стран и разведывательных служб конкурирующих отечественных и зарубежных предприятий;

— лица из криминальных структур, хакеры.

В части соотношения с видами и способами дестабилизирующего воздействия на информацию эти категории людей подразделяются на две группы: имеющие доступ к носителям данной защищаемой информации, техническим средствам ее отображения, хранения, обработки, воспроизведения, передачи и системам обеспечения их функционирования и не имеющие такового.

1.3. Практика №3. Моделирование процессов комплексной системы защиты информации. Нормативно-методическое обеспечение систем защиты информации. Управление комплексной системой защиты информации

1.3.1. Цель практической работы

Цель практической работы №3 состоит в рассмотрении принципов организации комплексных систем защиты информации.

1.3.2. Описание практической работы

Рассматриваются на практике аспекты моделирование процессов комплексной системы защиты информации и управления комплексной системой защиты информации.

Пример задач:

1. Рассмотреть общие принципы построения комплексной системы защиты информации.
2. Рассмотреть порядок развертывания системы защиты от несанкционированного доступа. Требования к системе защиты от несанкционированного доступа. Основные настройки системы защиты от несанкционированного доступа. Персонал, необходимый для администрирования системы защиты от несанкционированного доступа.
3. Рассмотреть порядок развертывания системы межсетевого экранирования. Требования к системе межсетевого экранирования. Основные настройки системы межсетевого экранирования. Персонал, необходимый для администрирования системы межсетевого экранирования.
4. Рассмотреть порядок развертывания системы обнаружения и предотвращения вторжений. Требования к системе обнаружения и предотвращения вторжений. Основные настройки системы обнаружения и предотвращения вторжений. Персонал, необходимый для администрирования системы обнаружения и предотвращения вторжений.
5. Рассмотреть порядок развертывания системы криптографической защиты информации. Требования к системе криптографической защиты информации. Основные настройки системы криптографической защиты информации. Персонал, необходимый

для администрирования системы криптографической защиты информации.

6. Рассмотреть порядок развертывания системы антивирусной защиты. Требования к системе антивирусной защиты. Основные настройки системы антивирусной защиты. Персонал, необходимый для администрирования системы антивирусной защиты.
7. Рассмотреть порядок развертывания системы мониторинга событий информационной безопасности. Требования к системе мониторинга событий информационной безопасности. Основные настройки системы мониторинга событий информационной безопасности. Персонал, необходимый для администрирования системы мониторинга событий информационной безопасности.

2. МЕТОДИЧЕСКИЕ УКАЗАНИЯ К ЛАБОРАТОРНЫМ РАБОТАМ

2.1 Лабораторная работа № 1. Предпроектное обследование. Аналитическое обоснование необходимости создания СЗИ.

2.1.1 Цели и задачи

Целью работы является ознакомление с общими принципами проведения предпроектного обследования.

Задачи:

1. Провести предпроектное обследование.
2. Сформировать отчет по итогам предпроектного обследования.
3. Обосновать необходимость внедрения СЗИ.

2.1.2 Теоретические положения

Целями предпроектного обследования являются:

- получение общей информации об объекте защиты;
- определение целей внедрения системы защиты;
- определение общих ключевых требований к системе защиты и границ проекта;
- определение общего состояния организации информационной безопасности;
- определение основных пользователей и администраторов системы защиты информации;
- определение общего уровня сложности системы защиты информации;
- оценка потребностей по внедрению системы защиты информации.

С целью получения необходимой информации об объекте защиты анкетирование и интервьюирование основных пользователей (Заказчика, руководителя проекта, руководителей подразделений, основных пользователей).

В результате проведения предпроектного обследования осуществляется:

- оценка объема работ, необходимых для внедрения системы защиты информации;
- анализ соответствия информационно-телекоммуникационной инфраструктуры требованиям информационной безопасности;
- подготовка отчета о проведенном предпроектном обследовании;
- подготовка и демонстрация прототипа решения (если необходимо);

Отчет о предпроектном обследовании может содержать разделы:

1 Сокращения, условные обозначения

2 Общие положения

2.1 Цель проведения аудита

После проведения предпроектного обследования становится возможным оценить объем аналитической и технической работ, которые потребуется провести, а также то, какие результаты должны быть достигнуты.

В результате разрабатывается документ, содержащий описание основных требований к системе защиты, границы проекта и другую выявленную информацию.

2.1.3 Порядок выполнения работы

1. Разработать план проведения обследования.
2. Составить опросные листы.
3. Собрать необходимую информацию.
4. Оформить отчет об обследовании.
5. Обосновать необходимость внедрения СЗИ.

2.1.4. Варианты заданий

Выполнить обследование системы ИИ, развернутой на:

1. 10 серверах, 15 АРМ, в 3 корпусах
2. 5 серверах, 5 АРМ, в 2 корпусах
3. 3 серверах, 30 АРМ, в 5 корпусах

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. Указать основной порядок проведения обследования.

2. Указать основные разделы отчета об обследовании.

3. 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. Техническое (частное техническое) задание на разработку СЗИ. Проектирование комплексной системы защиты информации

2.2.1 Цели и задачи

Целью работы является ознакомление с общими принципами проектирование КСЗИ.

Задачи:

1. Выявить требования к КСЗИ.

2. Выбрать технические решения, удовлетворяющие требованиям к КСЗИ.

2.2.2 Теоретические положения

Требования к системе защиты информации информационной системы включаются в техническое задание на создание информационной системы и (или) техническое задание (частное техническое задание) на создание системы защиты информации информационной системы, разрабатываемые с учетом ГОСТ 34.602, ГОСТ Р 51583 и ГОСТ Р 51624, и должны в том числе содержать:

- цель и задачи обеспечения защиты информации в информационной системе;
- класс защищенности информационной системы;
- перечень нормативных правовых актов, методических документов и национальных стандартов, которым должна соответствовать информационная система;
- перечень объектов защиты информационной системы;
- требования к мерам и средствам защиты информации, применяемым в информационной системе;
- стадии (этапы работ) создания системы защиты информационной системы;
- требования к поставляемым техническим средствам, программному обеспечению, средствам защиты информации;
- функции заказчика и оператора по обеспечению защиты информации в информационной системе;
- требования к защите средств и систем, обеспечивающих функционирование информационной системы (обеспечивающей инфраструктуре);
- требования к защите информации при информационном взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями, в том числе с информационными системами уполномоченного лица, а также при применении вычислительных ресурсов (мощностей), предоставляемых уполномоченным лицом для обработки информации.

При определении требований к системе защиты информации информационной системы учитываются положения политик обеспечения информационной безопасности обладателя информации (заказчика), а также политик обеспечения информационной безопасности оператора и

уполномоченного лица в части, не противоречащей политикам обладателя информации (заказчика).

В случае создания информационной системы, функционирование которой предполагается на базе информационно-телекоммуникационной инфраструктуры центра обработки данных, дополнительно определяются требования по защите информации, подлежащие реализации в информационно-телекоммуникационной инфраструктуре центра обработки данных.

Структура технического задания:

СОКРАЩЕНИЯ, УСЛОВНЫЕ ОБОЗНАЧЕНИЯ

1 ОБЩИЕ СВЕДЕНИЯ

1.1. Полное наименование системы и ее условное обозначение

1.2. Шифр темы

1.3. Наименование предприятий разработчика и заказчика Системы

1.4. Перечень документов, на основании которых создается Система

1.5. Плановые сроки начала и окончания работ по созданию Системы

1.6. Порядок оформления и предъявления результатов работ

2 НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ СИСТЕМЫ

2.1. Назначение Системы

2.2. Цели создания Системы

3 ХАРАКТЕРИСТИКА ОБЪЕКТА ЗАЩИТЫ

3.1. Краткие сведения об объекте защиты

3.1.1. Краткое описание ИС

3.1.2. Характеристики ИС

4 ТРЕБОВАНИЯ К СИСТЕМЕ

4.1. Требования к Системе в целом

4.1.1. Требования к структуре и функционированию Системы

4.1.2. Требования к численности и квалификации персонала Системы

4.1.3. Показатели назначения.

4.1.4. Требования к эксплуатации, техническому обслуживанию, ремонту и хранению компонентов Системы.

4.1.5. Требования по сохранности информации при авариях.

4.1.6. Требования к защите от влияния внешних воздействий.

4.1.7. Требования к патентной чистоте.

4.1.8. Требования по стандартизации и унификации.

4.1.9. Требования к размещению технических средств.

4.2. Требования к функциям, выполняемым Системой

4.2.1. Требования к подсистеме защиты от несанкционированного доступа.

4.2.2. Требования к подсистеме анализа защищенности.

4.2.3. Требования к подсистеме антивирусной защиты.

4.2.4. Требования к подсистеме безопасного межсетевого взаимодействия.

4.2.5. Требования к подсистеме регистрации событий информационной безопасности.

4.2.6. Организационно-технические требования.

4.3. Требования к видам обеспечения

4.3.1. Требования к программному обеспечению.

4.3.2. Требования к техническому обеспечению.

4.3.3. Требования к организационному обеспечению.

5 ТРЕБОВАНИЯ К СОСТАВУ И СОДЕРЖАНИЮ РАБОТ

5.1. В состав работ по обеспечению информационной безопасности информации, обрабатываемой в ИС, должны входить следующие мероприятия:

6 ПОРЯДОК КОНТРОЛЯ И ПРИЕМКИ СИСТЕМЫ

6.1. Виды, состав, объем и методы испытаний системы

6.2. Требования к аттестационным испытаниям системы в соответствии с требованиями по безопасности информации

6.3. Сведения об обслуживании системы

7 ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ

8 ПОРЯДОК ВНЕСЕНИЯ ИЗМЕНЕНИЙ

9 ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ИСТОЧНИКОВ

10 ПРИЛОЖЕНИЕ 1. СОСТАВ И СОДЕРЖАНИЕ МЕР ЗАЩИТЫ ИНФОРМАЦИИ

10.1. Определение базового набора мер защиты

10.2. Адаптация базового набора мер защиты

10.3. Уточнение адаптированного базового набора мер защиты

2.2.3 Порядок выполнения работы

1. Определение нормативных документов, которые необходимо использовать для формулирования требований.

2. Классификация защищаемой системы.

3. Выбор требований для данного класса системы ИИ.

4. Выбор основных технических решений по обеспечению ИБ системы ИИ.

2.2.4. Варианты заданий

Выполнить выбор технических решений для обеспечения ИБ системы ИИ, развернутой на:

1. 10 серверах, 15 АРМ, в 3 корпусах

2. 5 серверах, 5 АРМ, в 2 корпусах

3. 3 серверах, 30 АРМ, в 5 корпусах

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. Указать основной порядок формирования требований к КСЗИ.

2. Указать основной порядок формирования технических решений КСЗИ.

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

2.3 Лабораторная работа № 3. Технический проект КСЗИ

2.3.1 Цели и задачи

Целью работы является ознакомление с особенностями разработки технического проекта КСЗИ.

Задачи:

1. Сформировать структуру ТП КСЗИ.

2. Произвести наполнение ТП КСЗИ выбранными техническими решениями.

2.3.2 Теоретические положения

Разработка системы защиты информации информационной системы организуется обладателем информации (заказчиком).

Разработка системы защиты информации информационной системы осуществляется в соответствии с техническим заданием на создание информационной системы и (или) техническим заданием (частным техническим заданием) на создание системы защиты информации информационной системы с учетом ГОСТ 34.601 "Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания" (далее - ГОСТ 34.601), ГОСТ Р 51583 и ГОСТ Р 51624 и в том числе включает:

- проектирование системы защиты информации информационной системы;
- разработку эксплуатационной документации на систему защиты информации информационной системы;
- макетирование и тестирование системы защиты информации информационной системы (при необходимости).

Система защиты информации информационной системы не должна препятствовать достижению целей создания информационной системы и ее функционированию.

При разработке системы защиты информации информационной системы учитывается ее информационное взаимодействие с иными информационными системами и информационно-телекоммуникационными сетями, в том числе с информационными системами уполномоченного лица, а также применение вычислительных ресурсов (мощностей), предоставляемых уполномоченным лицом для обработки информации.

При проектировании системы защиты информации информационной системы:

- определяются типы субъектов доступа (пользователи, процессы и иные субъекты доступа) и объектов доступа, являющихся объектами защиты (устройства, объекты файловой системы, запускаемые и исполняемые модули, объекты системы управления

базами данных, объекты, создаваемые прикладным программным обеспечением, иные объекты доступа);

- определяются методы управления доступом (дискреционный, мандатный, ролевой или иные методы), типы доступа (чтение, запись, выполнение или иные типы доступа) и правила разграничения доступа субъектов доступа к объектам доступа (на основе списков, меток безопасности, ролей и иных правил), подлежащие реализации в информационной системе;
- выбираются меры защиты информации, подлежащие реализации в системе защиты информации информационной системы;
- определяются виды и типы средств защиты информации, обеспечивающие реализацию технических мер защиты информации;
- определяется структура системы защиты информации информационной системы, включая состав (количество) и места размещения ее элементов;
- осуществляется выбор средств защиты информации, сертифицированных на соответствие требованиям по безопасности информации, с учетом их стоимости, совместимости с информационными технологиями и техническими средствами, функций безопасности этих средств и особенностей их реализации, а также класса защищенности информационной системы;
- определяются требования к параметрам настройки программного обеспечения, включая программное обеспечение средств защиты информации, обеспечивающие реализацию мер защиты информации, а также устранение возможных уязвимостей информационной системы, приводящих к возникновению угроз безопасности информации;

- определяются меры защиты информации при информационном взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями, в том числе с информационными системами уполномоченного лица, а также при применении вычислительных ресурсов (мощностей), предоставляемых уполномоченным лицом для обработки информации.

Результаты проектирования системы защиты информации информационной системы отражаются в проектной документации (эскизном (техническом) проекте и (или) в рабочей документации) на информационную систему (систему защиты информации информационной системы), разрабатываемых с учетом ГОСТ 34.201 "Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем" (далее - ГОСТ 34.201).

Проектная документация на информационную систему и (или) ее систему защиты информации подлежат согласованию с оператором информационной системы в случае, если он определен таковым в соответствии с законодательством Российской Федерации к моменту окончания проектирования системы защиты информации информационной системы и не является заказчиком данной информационной системы.

При отсутствии необходимых средств защиты информации, сертифицированных на соответствие требованиям по безопасности информации, организуется разработка (доработка) средств защиты информации и их сертификация в соответствии с законодательством Российской Федерации или производится корректировка проектных решений по информационной системе и (или) ее системе защиты информации с учетом функциональных возможностей имеющихся сертифицированных средств защиты информации.

При проектировании системы защиты информации информационной системы, функционирование которой предполагается на базе информационно-телекоммуникационной инфраструктуры центра обработки данных, для блокирования актуальных угроз безопасности информации могут быть применены меры защиты информации, реализуемые в информационно-телекоммуникационной инфраструктуре центра обработки данных.

Разработка эксплуатационной документации на систему защиты информации информационной системы осуществляется в соответствии с техническим заданием на создание информационной системы и (или) техническим заданием (частным техническим заданием) на создание системы защиты информации информационной системы.

Эксплуатационная документация на систему защиты информации информационной системы разрабатывается с учетом ГОСТ 34.601, ГОСТ 34.201 и ГОСТ Р 51624 и должна в том числе содержать описание:

- структуры системы защиты информации информационной системы;
- состава, мест установки, параметров и порядка настройки средств защиты информации, программного обеспечения и технических средств;
- правил эксплуатации системы защиты информации информационной системы.

При макетировании и тестировании системы защиты информации информационной системы в том числе осуществляются:

- проверка работоспособности и совместимости выбранных средств защиты информации с информационными технологиями и техническими средствами;

- проверка выполнения выбранными средствами защиты информации требований к системе защиты информации информационной системы;
- корректировка проектных решений, разработанных при создании информационной системы и (или) системы защиты информации информационной системы;

Макетирование системы защиты информации информационной системы и ее тестирование может проводиться в том числе с использованием средств и методов моделирования информационных систем и технологий виртуализации.

Структура ТП КСЗИ:

4.3 Режимы функционирования КСЗИ

4.3.1 Решения по режимам функционирования КСЗИ

4.3.2 Решения по диагностированию работы КСЗИ

4.4 Численность, функции и квалификация персонала

4.4.1 Численность персонала КСЗИ

4.4.2 Квалификация обслуживающего персонала КСЗИ

4.4.3 Режим работы персонала КСЗИ

4.4.4 Квалификация пользователей КСЗИ

4.4.5 Режим работы пользователей КСЗИ

4.5 Обеспечение потребительских характеристик КСЗИ

4.5.1 Надежность КСЗИ

4.5.2 Безопасность обслуживающего персонала

4.6 Функции, выполняемые КСЗИ

4.6.1 Подсистема защиты от несанкционированного доступа

4.6.2 Подсистема анализа защищенности

4.6.3 Подсистема антивирусной защиты

4.6.4 Подсистема безопасного межсетевого взаимодействия

4.6.5 Подсистема регистрации событий

4.6.6 Подсистема управления

4.6.7 Решения по резервному копированию и восстановлению информации

4.6.8 Решения по выполнению требований технического заданий

4.7 Перечень требований к сторонним организациям для взаимодействия с ИС.

4.7.1 Требования к сетевому взаимодействию

4.7.2 Требования к защите от НСД

4.7.3 Требования к антивирусной защите

4.8 Описание комплекса технических средств

4.9 Сведения о сертификации

5 ОПИСАНИЕ МЕРОПРИЯТИЯ ПО ПОДГОТОВКЕ ОБЪЕКТА АВТОМАТИЗАЦИИ К ВВОДУ СИСТЕМЫ В ДЕЙСТВИЕ

5.1 Приведение информации к виду, пригодному для обработки на ЭВМ

5.2 Мероприятия по подготовке персонала

5.3 Организация необходимых подразделений и рабочих мест

5.4 Изменение объекта автоматизации

5.5 Дополнительные мероприятия

2.3.3 Порядок выполнения работы

1. Формирование структуры ТП КСЗИ.

2. Описание технических решений, сгруппированных по подсистемам.

3. Оформление необходимых схем.

2.3.4. Варианты заданий

Выполнить оформление ТП КСЗИ для обеспечения ИБ системы ИИ, развернутой на:

1. 10 серверах, 15 АРМ, в 3 корпусах

2. 5 серверах, 5 АРМ, в 2 корпусах

3. 3 серверах, 30 АРМ, в 5 корпусах

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. Указать основной порядок формирования ТП КСЗИ.

2. Указать основное содержание разделов ТП КСЗИ.

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

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 технических решений по обеспечению ИБ систем искусственного интеллекта.

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.

2) Определение актуальных угроз безопасности информации.

3) Определение требований к системе защиты.

4) Выбор технических решений системы защиты.

5) Выбор средств защиты информации.

6) Определение необходимого набора организационно-распорядительных документов.

3.3. Примерные варианты заданий контрольной работы

Примерный список вариантов контрольной работы:

1. Разработка модели угроз и нарушителя для типовой системы искусственного интеллекта

2. Разработка технического задания на систему защиты для типовой системы искусственного интеллекта

3. Разработка ответа о предпроектном обследовании для типовой системы искусственного интеллекта

4. Разработка технического проекта для типовой системы искусственного интеллекта

ЗАКЛЮЧЕНИЕ

В рамках курса на практических примерах и в лабораторном практикуме рассматриваются общие вопросы обеспечения безопасности систем 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

Безопасность систем искусственного интеллекта

Учебное пособие

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