

Документ подписан простой электронной подписью  
Информация о владельце:  
ФИО: Баламирзоев Назим Лиодинович  
Должность: Ректор  
Дата подписания: 04.12.2024 10:08  
Уникальный программный ключ:  
5cf0d6f89e80f49a334f6a4ba58e91f3326b9926

Министерство науки и высшего образования РФ

Федеральное государственное бюджетное образовательное учреждение  
высшего образования

«Дагестанский государственный технический университет»

## РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Дисциплина «Технологии построения защищённых автоматизированных систем»

наименование дисциплины по ОПОП

для направления (специальности) 10.03.01 Информационная безопасность  
код и полное наименование направления (специальности)

по профилю (специализации, программе) Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности),

факультет Компьютерных технологий и энергетики,  
наименование факультета, где ведется дисциплина

кафедра Информационная безопасность.  
наименование кафедры, за которой закреплена дисциплина

Форма обучения очная, очно-заочная, курс 3 (4), семестр (ы) 6 (7).  
очная, очно-заочная, заочная

г. Махачкала 2024

Программа составлена в соответствии с требованиями ФГОС ВО по направлению 10.03.01 Информационная безопасность с учетом рекомендаций и ОПОП ВО по направлению 10.03.01 Информационная безопасность и профилю Безопасность автоматизированных систем.

/Разработчик  Каннер Т.М., старший преподаватель кафедры защиты информации МФТИ  
подпись (ФИО уч. степень, уч. звание)

«27» сентября 2024г.

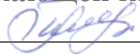
**Зав. кафедрой, за которой закреплена дисциплина (модуль) ТПЗАС**

 Качаева Г. И., к.э.н., доцент  
подпись (ФИО уч. степень, уч. звание)

«27» сентября 2024г.

Программа одобрена на заседании выпускающей кафедры Информационная безопасность от 15 октября 2024года, протокол № 3.

**Зав. выпускающей кафедрой по данному направлению (специальности, профилю)**

 Качаева Г. И., к.э.н., доцент  
подпись (ФИО уч. степень, уч. звание)

«15» октября 2024 г.

Программа одобрена на заседании Методического Совета факультета компьютерных технологий и энергетики от 17 октября 2024года, протокол № 2.

**Председатель Методического совета факультета КТиЭ**

  
подпись

Т.И. Исабекова, к.ф.-м.н., доцент  
(ФИО уч. степень, уч. звание)

**Декан факультета**

  
подпись

Т.А. Рагимова  
ФИО

**Начальник УО**

  
подпись

М.Т. Муталибов  
ФИО

**Проректор по УР**

  
подпись

А.Ф. Демирова  
ФИО

## **1. Цели и задачи освоения дисциплины.**

Целью освоения дисциплины «Технологии построения защищённых автоматизированных систем» является формирование у студентов знаний основ технологий проектирования, построения и создания защищённых автоматизированных систем, а также навыков и умений в применении знаний для конкретных условий. Кроме того, целью дисциплины является развитие в процессе обучения системного мышления, необходимого для решения задач защиты информации с учётом требований системного подхода.

Задачи дисциплины:

- получение представлений о принципах построения защищённых автоматизированных систем;
- знакомство с современными защищёнными автоматизированными системами.

## **2. Место дисциплины в структуре ОПОП**

Дисциплина относится к обязательной части образовательной программы.

Дисциплина базируется на следующих дисциплинах ОПОП:

- Основы информационной безопасности;
- Операционные системы;
- Безопасность систем баз данных;
- Теоретические основы компьютерной безопасности.

Требования к «входным» знаниям, умениям и готовностям, необходимым при освоении дисциплины и приобретенным в результате освоения предшествующих дисциплин:

- знание базовых понятий области обеспечения информационной безопасности;
- знание базовых понятий операционных систем различных видов;
- знание принципов построения операционных систем различных видов;
- знание базовых понятий компьютерной безопасности;
- умение работать с операционными системами различных видов;
- готовность совершенствовать полученные умения по работе с операционными системами различных видов для установки, настройки и администрирования программно-аппаратных СЗИ.

Дисциплина предшествует изучению следующих дисциплин ОПОП:

- Методы оценки безопасности компьютерных систем;
- Информационная безопасность открытых систем;
- Комплексное обеспечение информационной безопасности автоматизированных систем.

### 3. Компетенции обучающегося, формируемые в результате освоения дисциплины

В результате освоения дисциплины «Технологии построения защищённых АС» студент должен овладеть следующими компетенциями: (перечень компетенций и индикаторов их достижения относящихся к дисциплинам, указан в соответствующей ОПОП).

| Код компетенции | Наименование компетенции                                                                                                                                                     | Наименование показателя оценивания (показатели достижения заданного уровня освоения компетенций)                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| УК-1            | Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач                                               | УК-1.3 - знает основные источники информации о проблемных ситуациях в профессиональной деятельности и подходы к критическому анализу этой информации<br>УК-1.4 - знает порядок принятия решений при возникновении проблемных ситуаций в профессиональной деятельности<br>УК-1.5 - умеет критически анализировать проблемные ситуации и вырабатывать стратегию действий в ходе решения профессиональных задач                                                                         |
| УК-2            | Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений   | УК-2.2- умеет разрабатывать и реализовывать этапы проекта в сфере профессиональной деятельности                                                                                                                                                                                                                                                                                                                                                                                      |
| УК-6            | Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни                                  | УК-6.1 знает методы и средства самостоятельного решения задач в сфере профессиональной деятельности                                                                                                                                                                                                                                                                                                                                                                                  |
| ОПК-5           | Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности | ОПК-5.1 - знает основы законодательства Российской Федерации, систему нормативных правовых актов, нормативных и методических документов в области информационной безопасности и защиты информации<br>ОПК-5.2 - знает правовые основы организации защиты персональных данных и охраны результатов интеллектуальной деятельности<br>ОПК-5.5 - умеет формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной |

|         |                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|         |                                                                                                                                                                                                                                                                                                              | деятельности в организации                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| ОПК-6   | Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю. | ОПК-6.5 - умеет определить политику контроля доступа работников к информации ограниченного доступа<br>ОПК-6.6 - умеет формулировать основные требования, предъявляемые к физической защите объекта и пропускному режиму в организации                                                                                                                                                                                                                                                                       |
| ОПК-9   | Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности.                                                                                                                                                                               | ОПК-9.4 - умеет использовать СКЗИ для решения задач профессиональной деятельности                                                                                                                                                                                                                                                                                                                                                                                                                           |
| ОПК-10  | ОПК-10. Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты.                          | ОПК-10.1 - знает программно-аппаратные средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях<br>ОПК-10.8 - знает принципы организации информационных систем в соответствии с требованиями по защите информации<br>ОПК-10.9 - знает особенности комплексного подхода к обеспечению информационной безопасности организации<br>ОПК-10.10 - умеет определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите |
| ОПК 4.1 | Способен проводить организационные мероприятия по обеспечению безопасности информации в автоматизированных системах.                                                                                                                                                                                         | ОПК-4.1.1. Знает задачи программно-технического обеспечения информационной безопасности в организации и политику безопасности в операционных системах.<br>ОПК-4.1.5. Владеет навыками разработки и применения системы безопасности, прикладными и инструментальными средствами создания систем информационной безопасности.                                                                                                                                                                                 |
| ОПК 4.4 | Способен осуществлять диагностику и мониторинг систем защиты автоматизированных систем.                                                                                                                                                                                                                      | ОПК-4.1.1. Знает задачи программно-технического обеспечения информационной безопасности в организации и политику безопасности в операционных                                                                                                                                                                                                                                                                                                                                                                |

|  |  |                                                                                                                                                                                |
|--|--|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  |  | системах.<br>ОПК-4.1.5. Владеет навыками разработки и применения системы безопасности, прикладными и инструментальными средствами создания систем информационной безопасности. |
|--|--|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### 4. Объем и содержание дисциплины (модуля)

| <b>Форма обучения</b>                                                                                                     | <b>очная</b> | <b>очно-заочная</b> | <b>заочная</b> |
|---------------------------------------------------------------------------------------------------------------------------|--------------|---------------------|----------------|
| <i>Общая трудоемкость по дисциплине (ЗЕТ/ в часах)</i>                                                                    | <i>3/108</i> | <i>3/108</i>        | —              |
| <i>Семестр</i>                                                                                                            | <i>6</i>     | <i>7</i>            | —              |
| <i>Лекции, час</i>                                                                                                        | <i>34</i>    | <i>17</i>           | —              |
| <i>Практические занятия, час</i>                                                                                          | —            | —                   | —              |
| <i>Лабораторные занятия, час</i>                                                                                          | <i>34</i>    | <i>17</i>           | —              |
| <i>Самостоятельная работа, час</i>                                                                                        | <i>40</i>    | <i>74</i>           | —              |
| <i>Курсовой проект (работа), РГР, семестр</i>                                                                             | —            | —                   | —              |
| <i>Зачет (при заочной форме 4 часа отводится на контроль)</i>                                                             | +            | <i>4 часа</i>       | —              |
| <i>Часы на экзамен (при очной, очно-заочной формах 1 ЗЕТ – 36 часов, при заочной форме 9 часов отводится на контроль)</i> | -            | —                   | —              |

#### 4.1.Содержание дисциплины (модуля)

| №<br>п/п                                                            | Раздел дисциплины, тема лекции и вопросы                                                                                                                                                                                                 | Очная форма |    |    |    | Очно-заочная форма |    |    |    | Заочная форма |    |    |    |
|---------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|----|----|----|--------------------|----|----|----|---------------|----|----|----|
|                                                                     |                                                                                                                                                                                                                                          | ЛК          | ПЗ | ЛБ | СР | ЛК                 | ПЗ | ЛБ | СР | ЛК            | ПЗ | ЛБ | СР |
| Раздел 1. Введение в предмет.                                       |                                                                                                                                                                                                                                          |             |    |    |    |                    |    |    |    |               |    |    |    |
| 1                                                                   | Автоматизированные системы: основные термины и определения. Жизненный цикл АС. Понятие защищённой АС. Подходы к созданию защищённых АС. Проблемы проектирования и реализации защищённых АС.                                              | 2           | –  | 2  | 2  | 1                  | –  | 4  | –  | –             | –  | –  | –  |
| 2                                                                   | Подход к среде функционирования АС. Технические средства обеспечения доверенной среды.                                                                                                                                                   | 2           | –  | 2  | 2  | 1                  | –  | 5  | –  | –             | –  | –  | –  |
| 3                                                                   | Меры по обеспечению безопасности информации в ГИС. Требования к защите АС.                                                                                                                                                               | 2           | –  | 2  | 2  | 1                  | –  | 5  | –  | –             | –  | –  | –  |
| Раздел 2. Персональные средства криптографической защиты информации |                                                                                                                                                                                                                                          |             |    |    |    |                    |    |    |    |               |    |    |    |
| 4                                                                   | Персональные СКЗИ. Проблемы использования и примеры решений. Проблемы использования СКЗИ на планшетах. Защищённые носители вычислительной среды. Защищённые носители ключевой и аутентификационной информации.                           | 2           | –  | 2  | 2  | 1                  | –  | 5  | –  | –             | –  | –  | –  |
| Раздел 3. Технологии безопасного терминального доступа              |                                                                                                                                                                                                                                          |             |    |    |    |                    |    |    |    |               |    |    |    |
| 5                                                                   | Инструменты контроля доступа для организации удалённой работы. Обеспечение безопасности и распределение ответственности при организации удалённого доступа. Защита ИСПДн с применением технологии терминального доступа.                 | 2           | –  | 2  | 2  | 1                  | –  | 5  | –  | –             | –  | –  | –  |
| Раздел 4. Технологии защиты систем виртуализации                    |                                                                                                                                                                                                                                          |             |    |    |    |                    |    |    |    |               |    |    |    |
| 6                                                                   | Системы виртуализации: состав и особенности функционирования. Особенности защиты виртуальных машин. Доверенная загрузка и контроль целостности систем виртуализации. Средства защиты систем виртуализации для гипервизоров KVM и VMware. | 2           | –  | 2  | 3  | 1                  | –  | 5  | –  | –             | –  | –  | –  |

|                                                                                                       |                                                                                                                                                                                                                                                                                                  |   |   |   |   |   |   |   |   |   |   |   |   |
|-------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|---|---|---|---|---|---|---|---|---|
| 7                                                                                                     | Инфраструктура безопасного «облака». Контейнеризация. Особенности и инструменты защиты контейнеров.                                                                                                                                                                                              | 2 | – | 2 | 3 | 1 | – | 5 | – | – | – | – | – |
| <i>Раздел 5. Доверенная интеграционная платформа и стек технологий физической безопасности</i>        |                                                                                                                                                                                                                                                                                                  |   |   |   |   |   |   |   |   |   |   |   |   |
| 8                                                                                                     | Особенности размещения СВТ вне контролируемой зоны: организационно-правовые и технические аспекты.                                                                                                                                                                                               | 2 | – | 2 | 3 | 1 | – | 5 | – | – | – | – | – |
| 9                                                                                                     | Доверенная интеграционная платформа: состав и назначение. Модель угроз и модель нарушителя. Методы и средства защиты комплекса технических средств от инвазивных воздействий. Защищённые стойки. Идентификация и аутентификация. Подсистемы видеонаблюдения и охранной сигнализации.             | 2 | – | 2 | 3 | 1 | – | 5 | – | – | – | – | – |
| <i>Раздел 6. Технологии слепой обработки привлекаемых данных в системах искусственного интеллекта</i> |                                                                                                                                                                                                                                                                                                  |   |   |   |   |   |   |   |   |   |   |   |   |
| 10                                                                                                    | Слепая обработка данных в системах ИИ. Организация доверия участников к системе. СВТ в защищённом исполнении как часть АС: состав и назначение. Взаимодействие участников АС с СВТ ЗИ. Оповещение участников о нештатных ситуациях. Организация дистанционного голосования по ключевым вопросам. | 2 | – | 2 | 3 | 1 | – | 5 | – | – | – | – | – |
| 11                                                                                                    | Методы и средства защиты данных, размещённых в АС от неинвазивных воздействий. Методы и средства защиты данных, размещённых в АС от инвазивных воздействий. Методы контроля криптографических ключей в СВТ ЗИ.                                                                                   | 2 | – | 2 | 3 | 1 | – | 5 | – | – | – | – | – |
| <i>Раздел 7. Технические средства биометрической защиты.</i>                                          |                                                                                                                                                                                                                                                                                                  |   |   |   |   |   |   |   |   |   |   |   |   |
| 12                                                                                                    | Классические средства биометрической защиты. Новая биометрия. Замысел защиты.                                                                                                                                                                                                                    | 3 | – | 3 | 3 | 1 | – | 5 | – | – | – | – | – |
| 13                                                                                                    | Технические решения на базе новой биометрии. Перспективы развития.                                                                                                                                                                                                                               | 3 | – | 3 | 3 | 1 | – | 5 | – | – | – | – | – |
| <i>Раздел 8. Системы видеонаблюдения и контроля доступа</i>                                           |                                                                                                                                                                                                                                                                                                  |   |   |   |   |   |   |   |   |   |   |   |   |
| 14                                                                                                    | Методы контроля доступа. Общие принципы построения СВКД. Интеграция подсистемы информационной безопасности в общую ИС.                                                                                                                                                                           | 3 | – | 3 | 3 | 2 | – | 5 | – | – | – | – | – |
| 15                                                                                                    | Интеграция СЗИ НСД и СКУД. Интеграция СЗИ НСД и системы видеомониторинга и контроля доступа.                                                                                                                                                                                                     | 3 | – | 3 | 3 | 2 | – | 5 | – | – | – | – | – |



|                                                                                |                                                                                                                                   |  |           |           |                                                                                                                                   |  |           |           |                                          |  |  |  |
|--------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|--|-----------|-----------|-----------------------------------------------------------------------------------------------------------------------------------|--|-----------|-----------|------------------------------------------|--|--|--|
| Форма текущего контроля успеваемости (по срокам текущих аттестаций в семестре) | Входной контроль<br>1 аттестация 1-5 тема – Опрос № 1<br>2 аттестация 6-9 тема – Опрос № 2<br>3 аттестация 10-15 тема – Опрос № 3 |  |           |           | Входной контроль<br>1 аттестация 1-5 тема – Опрос № 1<br>2 аттестация 6-9 тема – Опрос № 2<br>3 аттестация 10-15 тема – Опрос № 3 |  |           |           | –                                        |  |  |  |
| Форма промежуточной аттестации (по семестрам)                                  | Зачет                                                                                                                             |  |           |           | зачет                                                                                                                             |  |           |           | <del>Зачет/зачет с оценкой/экзамен</del> |  |  |  |
| <b>Итого</b>                                                                   | <b>34</b>                                                                                                                         |  | <b>34</b> | <b>40</b> | <b>17</b>                                                                                                                         |  | <b>17</b> | <b>74</b> |                                          |  |  |  |

#### 4.2. Содержание лабораторных (практических) занятий

| № п/п | № лекции из рабочей программы | Наименование лабораторного (практического, семинарского) занятия                                                                                                                                           | Количество часов |             |        | Рекомендуемая литература и методические разработки (№ источника из списка литературы) |
|-------|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|-------------|--------|---------------------------------------------------------------------------------------|
|       |                               |                                                                                                                                                                                                            | Очно             | Очно-заочно | Заочно |                                                                                       |
| 1     | 2                             | 3                                                                                                                                                                                                          | 4                | 5           | 6      | 7                                                                                     |
| 1     | 2                             | Настройка и администрирование ПАК «МАРШ!»                                                                                                                                                                  | 4                | 2           | –      | 4                                                                                     |
| 2     | 4                             | Настройка и администрирование «Идеального токена». Настройка и администрирование ПАК «ПИ ШИПКА».                                                                                                           | 6                | 2           | –      | 4                                                                                     |
| 3     | 5                             | Установка, настройка и администрирование ПАК «Центр-Т».                                                                                                                                                    | 6                | 4           | –      | 4                                                                                     |
| 4     | 5                             | Установка, настройка и администрирование защищённых терминалов «m-TrusT».                                                                                                                                  | 6                | 2           | –      | 4                                                                                     |
| 5     | 6                             | Установка, настройка и администрирование защиты систем виртуализации для KVM («Аккорд-KVM»). Установка, настройка и администрирование защиты систем виртуализации для VMware («Аккорд-В.» и «Сегмент-В.»). | 6                | 2           |        | 4                                                                                     |
| 6     | 10, 11                        | Ознакомление с АС «Анклав». Загрузка и обработка данных. Настройка параметров физической защиты.                                                                                                           | 6                | 4           | –      |                                                                                       |
| ИТОГО |                               |                                                                                                                                                                                                            | 34               | 4           | –      | –                                                                                     |

#### 4.3. Тематика для самостоятельной работы студента

| №<br>п/п | Тематика по содержанию дисциплины, выделенная для самостоятельного изучения                                        | Количество часов из содержания дисциплины |             |        | Рекомендуемая литература и источники информации | Формы контроля СРС |
|----------|--------------------------------------------------------------------------------------------------------------------|-------------------------------------------|-------------|--------|-------------------------------------------------|--------------------|
|          |                                                                                                                    | Очно                                      | Очно-заочно | Заочно |                                                 |                    |
| 1        | 2                                                                                                                  | 3                                         | 4           | 5      |                                                 |                    |
| 1        | Постановка проблемы комплексного обеспечения информационной безопасности АС.                                       | 4                                         | 8           | –      | 3                                               | Устный опрос       |
| 2        | Классические архитектуры: фон-Неймана и Гарвардская. НГА. Отличия от классических архитектур.                      | 4                                         | 8           | –      | 3                                               | Устный опрос       |
| 3        | Защищённые носители вычислительной среды. Доверенный сеанс связи.                                                  | 4                                         | 8           | –      | 3                                               | Устный опрос       |
| 4        | Защита ИСПДн с применением технологии терминального доступа.                                                       | 4                                         | 8           | –      | 3                                               | Устный опрос       |
| 5        | Защита от НСД физических и виртуальных машин: общее и отличия.                                                     | 4                                         | 8           | –      | 1, 4                                            | Устный опрос       |
| 6        | Идентификация и аутентификация. Факторы аутентификации: классификация и применение.                                | 4                                         | 8           | –      | 1, 3, 4                                         | Устный опрос       |
| 7        | Особенности размещения СВТ ЗИ вне контролируемой зоны.                                                             | 4                                         | 8           | –      | 3, 4                                            | Устный опрос       |
| 8        | Преимущества и недостатки «новой» биометрии по сравнению с классической.                                           | 6                                         | 8           | –      | 3                                               | Устный опрос       |
| 9        | Дискреционная, мандатная и ролевая модели разграничения доступа. Особенности применения, достоинства и недостатки. | 6                                         | 10          | –      | 1, 3                                            | Устный опрос       |
| ИТОГО    |                                                                                                                    | 40                                        | 74          | –      | –                                               | Зачет              |

### *5. Образовательные технологии*

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю):

- дистанционные технологии;
- электронные средства обучения;
- мастер-классы;
- мультимедийные технологии.

### **6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины**

В рамках дисциплины (модуля) предусмотрено 3 (три) аттестации текущего контроля успеваемости и промежуточная аттестация.

Каждый текущий контроль успеваемости представляет собой контрольную работу в форме тестирования. Выполнение СРС контролируется путем устного опроса по изученному материалу.

Промежуточная аттестация представляет собой зачет с устным ответом на 2 случайно выбранных вопроса из перечня вопросов для подготовки к промежуточной аттестации (вопросов для проведения зачета).

Эссе, рефераты и курсовые работы в рамках дисциплины (модуля) не предусмотрены.

Фонд оценочных средств приведен в Приложении А к настоящей РПД.

**7. Учебно-методическое и информационное обеспечение дисциплины**  
**Рекомендуемая литература и источники информации (основная и дополнительная)**

Зав. библиотекой \_\_\_\_\_



Сулейманова О.Ш.

(подпись)

| №<br>п/п                  | Виды<br>занятий | Необходимая учебная,<br>учебно-методическая<br>(основная и<br>дополнительная)<br>литература,<br>программное<br>обеспечение,<br>электронно-<br>библиотечные и<br>Интернет ресурсы                          | Автор(ы)                                               | Издательс<br>тво и год<br>издания | Количество изданий                        |   |
|---------------------------|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------|-----------------------------------|-------------------------------------------|---|
|                           |                 |                                                                                                                                                                                                           |                                                        |                                   | В библиотеке                              |   |
| 1                         | 2               | 3                                                                                                                                                                                                         | 4                                                      | 5                                 | 6                                         | 7 |
| Основная литература       |                 |                                                                                                                                                                                                           |                                                        |                                   |                                           |   |
| 1                         | ЛК, СР          | Управление защитой информации на базе СЗИ НСД «Аккорд»                                                                                                                                                    | Коняевский В.А.                                        | Радио и связь, 1999               | URL:<br>https://e.lanbook.com/book/72890  |   |
| 2                         | ЛК, СР          | Программно-аппаратные средства обеспечения информационной безопасности                                                                                                                                    | Душкин А.В., Барсуков О.М., Кравцов Е.В., Славнов К.В. | Горячая линия-Телеком, 2023       | URL:<br>https://e.lanbook.com/book/111084 |   |
| 3                         | ЛК, ЛБ, СР      | Доверенные информационные технологии: от архитектуры к системам и средствам                                                                                                                               | Коняевский В. А., Коняевская С.В.                      | URSS, 2021                        | URL:<br>https://e.lanbook.com/book/120059 |   |
| 4                         | ЛК, ЛБ, СР      | Платформенные решения ОКБ САПР как основа построения защищенных ИС.<br>URL:<br>https://www.okbsapr.ru/library/publications/platformennye-resheniya-okb-sapr-kak-osnova-postroeniya-zashchishchennykh-is1/ | Каннер Т.М.                                            | Медиа Группа «Авангард», 2020     | URL:<br>https://e.lanbook.com/book/72890  |   |
| 5                         | ЛК, СР          | Сайт ФСТЭК России.<br>URL: https://fstec.ru/                                                                                                                                                              | –                                                      | –                                 | fstec.ru                                  |   |
| Дополнительная литература |                 |                                                                                                                                                                                                           |                                                        |                                   |                                           |   |
| 6                         | ЛК, ЛБ, СР      | Компьютерная преступность. Т. I, II.                                                                                                                                                                      | Коняевский В.А., Лопаткин С.В.                         | РФК-Имидж Лаб, 2006               | URL:<br>https://e.lanbook.com/book/60868  |   |
| 7                         | ЛБ, СР          | Дистанционный курс                                                                                                                                                                                        | Каннер Т.М.                                            | 2024                              | URL:                                      |   |

|   |        |                                                                                                                                                                                                                                   |                          |                             |                                                                                           |
|---|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|-----------------------------|-------------------------------------------------------------------------------------------|
|   |        | «Меры и средства защиты информации от НСД»<br>URL:<br><a href="https://www.okbsapr.ru/education/mery-i-sredstva-zashchity-informatsii-ot-nsd/">https://www.okbsapr.ru/education/mery-i-sredstva-zashchity-informatsii-ot-nsd/</a> |                          |                             | <a href="https://e.lanbook.com/book/254480">https://e.lanbook.com/book/254480</a>         |
| 8 | ЛК, СР | Методология оценки эффективности защиты информации в информационных системах от несанкционированного доступа                                                                                                                      | Язов Ю.К., Соловьев С.В. | Наукоёмкие технологии, 2023 | URL:<br><a href="https://e.lanbook.com/book/247967">https://e.lanbook.com/book/247967</a> |
| 9 | ЛК, СР | Организация защиты информации в информационных системах от несанкционированного доступа                                                                                                                                           | Язов Ю.К., Соловьев С.В. | Кварта, 2018                | URL:<br><a href="https://e.lanbook.com/book/110053">https://e.lanbook.com/book/110053</a> |

#### **8. Материально-техническое обеспечение дисциплины (модуля)\_\_\_\_\_**

Учебная аудитория дисциплины (модуля) «Технологии построения защищённых АС» оснащена следующим учебно-лабораторным оборудованием:

- ПК преподавателя с ОС Windows с установленной программой просмотра документов в формате pdf (например, Adobe Acrobat Reader DC) и программой виртуализации (например, VirtualBox), средствами организации дистанционного обучения;
- мультимедийное оборудование, доска;
- ПК студентов с ОС Windows с установленной программой просмотра документов в формате pdf (например, Adobe Acrobat Reader DC) и программой виртуализации (например, VirtualBox);
- программно-аппаратные средства обеспечения информационной безопасности: СЗИ НСД «Аккорд-АМДЗ», СОДС «МАРШ!», «m-TruST», ПАК «ПИ ШИПКА», СЗИ «Аккорд-В.», СЗИ «Аккорд-KVM», СДЗ «Сегмент-В.», ПАК «Центр-Т», СВТ ЗИ «Анклав».

#### **Специальные условия инвалидам и лицам с ограниченными возможностями здоровья (ОВЗ)**

Специальные условия обучения и направления работы с инвалидами и лицами с ОВЗ определены на основании:

- Федерального закона от 29.12.2012 №273-ФЗ «Об образовании в Российской Федерации»;
- Федерального закона от 24.11.1995 № 181-ФЗ «О социальной защите инвалидов в Российской Федерации»;
- приказа Минобрнауки России от 05.04.2017 № 301 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры»;
- методических рекомендаций по организации образовательного процесса для обучения инвалидов и лиц с ограниченными возможностями здоровья в образовательных организациях высшего образования, в том числе оснащенности образовательного процесса, утвержденных Минобрнауки России 08.04.2014 № АК-44/05вн).

Под специальными условиями для получения образования обучающихся с ОВЗ понимаются условия обучения, воспитания и развития, включающие в себя использование при необходимости адаптированных образовательных программ и методов обучения и воспитания, специальных учебников, учебных пособий и дидактических материалов, специальных технических средств обучения коллективного и индивидуального пользования, предоставление услуг ассистента (помощника), оказывающего необходимую помощь, проведение групповых и индивидуальных коррекционных занятий, обеспечение доступа в здания ДГТУ и другие условия, без которых невозможно или затруднено освоение ОПОП обучающихся с ОВЗ.

Обучение в рамках учебной дисциплины обучающихся с ОВЗ осуществляется ДГТУ с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

Обучение по учебной дисциплине обучающихся с ОВЗ может быть организовано как совместно с другими обучающимися, так и в отдельных группах.

В целях доступности обучения по дисциплине обеспечивается:

1) для лиц с ограниченными возможностями здоровья по зрению:

- наличие альтернативной версии официального сайта ДГТУ в сети «Интернет» для слабовидящих;

- весь необходимый для изучения материал, согласно учебному плану (в том числе, для обучающихся по индивидуальным учебным планам) предоставляется в электронном виде на диске.

- индивидуальное равномерное освещение не менее 300 люкс;

- присутствие ассистента, оказывающего обучающемуся необходимую помощь;

- обеспечение возможности выпуска альтернативных форматов печатных материалов (крупный шрифт или аудиофайлы);

- обеспечение доступа обучающегося, являющегося слепым и использующего собаку-проводника, к зданию ДГТУ.

2) для лиц с ОВЗ по слуху:

- наличие микрофонов и звукоусиливающей аппаратуры коллективного пользования (аудиоколонки);

3) для лиц с ОВЗ, имеющих нарушения опорно-двигательного аппарата, материально-технические условия должны обеспечивать возможность беспрепятственного доступа обучающихся в учебные помещения, столовые, туалетные и другие помещения организации, а также пребывания в указанных помещениях (наличие пандусов, поручней, расширенных дверных проемов и других приспособлений).

Перед началом обучения могут проводиться консультативные занятия, позволяющие студентам с ОВЗ адаптироваться к учебному процессу.

В процессе ведения учебной дисциплины научно-педагогическим работникам рекомендуется использование социально-активных и рефлексивных методов обучения, технологий социокультурной реабилитации с целью оказания помощи обучающимся с ОВЗ в установлении полноценных межличностных отношений с другими обучающимися, создании комфортного психологического климата в учебной группе.

Особенности проведения текущей и промежуточной аттестации по дисциплине для обучающихся с ОВЗ устанавливаются с учетом индивидуальных психофизических особенностей (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и др.). При необходимости предоставляется дополнительное время для подготовки ответа на зачете или экзамене.