

**Минобрнауки России**  
**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ**  
**ВЫСШЕГО ОБРАЗОВАНИЯ**  
**«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНЖЕНЕРНЫХ ТЕХНОЛО-**  
**ГИЙ»**

**УТВЕРЖДАЮ**  
Проректор по учебной работе

\_\_\_\_\_  
(подпись)

Василенко В.Н.  
(Ф.И.О.)

«25» мая 2023

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

**Разработка и эксплуатация защищенных автоматизированных систем**

Специальность

10.05.03 Информационная безопасность автоматизированных систем

Специализация

Безопасность открытых информационных систем

Квалификация выпускника

специалист по защите информации

## 1. Цели и задачи дисциплины (модуля)

Целями освоения дисциплины «Разработка и эксплуатация защищенных автоматизированных систем» являются:

контрольно-аналитическая:

контроль работоспособности и эффективности применяемых средств защиты информации;

выполнение экспериментально-исследовательских работ при сертификации средств защиты информации и аттестации автоматизированных систем;

проведение инструментального мониторинга защищенности автоматизированных систем и анализа его результатов.

Объектами профессиональной деятельности являются:

– автоматизированные системы, функционирующие в условиях существования угроз в информационной сфере и обладающие информационно-технологическими ресурсами, подлежащими защите;

– информационные технологии, формирующие информационную инфраструктуру в условиях существования угроз в информационной сфере и задействующие информационно-технологические ресурсы, подлежащие защите;

– технологии обеспечения информационной безопасности автоматизированных систем;

– системы управления информационной безопасностью автоматизированных систем.

## 2. Перечень планируемых результатов обучения, соотнесенных с планируемыми результатами освоения образовательной программы

В результате освоения дисциплины в соответствии с предусмотренными компетенциями обучающийся должен:

| № п/п | Код компетенции | Содержание компетенции (результат освоения)  | В результате изучения учебной дисциплины обучающийся должен:   |  |   |
|-------|-----------------|--|--|--|---|
|       |                 |  | знать  | уметь  | владеть   |
| 1     | ОПК-6           | способностью применять нормативные правовые акты в профессиональной деятельности   | основы документооборота и основные нормативные правовые акты в области информационной безопасности, основные положения ФСТЭК РФ        | использовать методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных | навыками организации и использования при проведении работ по обеспечению безопасности персональных данных в автоматизированных информационных системах        |
| 2     | ПК-15           | способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем      | основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические) | восстанавливать работоспособность подсистемы информационной безопасности автоматизированных систем в нестандартных ситуациях                       | владеть навыками работы с современными инструментальными средствами для исследования программного обеспечения защищенных автоматизированных систем управления |
| 3     | ПК-20           | способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности | основы комплексного обеспечения информационной безопасности распределенных автоматизированных, информационно-управляющих систем        | решать практические задачи информационной безопасности на основе инфраструктуры открытых ключей  | навыками развертывания и обеспечения работы программных комплексов, обеспечивающих работу с цифровыми сертификатами   |

### 3. Место дисциплины (модуля) в структуре ОП ВО

Дисциплина «Разработка и эксплуатация защищенных автоматизированных систем» относится к блоку 1 ОП и ее базовой части.

Изучение дисциплины основано на знаниях, умениях и навыках, полученных при изучении обучающимися дисциплин:

- Организационное и правовое обеспечение информационной безопасности;
- Основы информационной безопасности;
- Система обнаружения компьютерных атак;
- Технологии разработки защищенного документооборота;
- Управление информационной безопасностью;
- Учебная практика, практика по получению первичных профессиональных умений;
- Производственная практика, практика по получению профессиональных умений и опыта профессиональной деятельности.

Дисциплина является предшествующей для изучения дисциплин:

- Аудит информационных технологий и систем обеспечения информационной безопасности;
- Безопасность облачных и распределенных вычислений;
- Гуманитарные аспекты информационной безопасности;
- Защита конфиденциальной информации;
- Производственная практика, преддипломная практика; защиты выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты.

### 4. Объем дисциплины (модуля) и виды учебных занятий

Общая трудоемкость дисциплины составляет 4 зачетных единицы.

| Виды учебной работы                                 | Всего часов | 9 семестр   |
|---|-------------|-------------|
| Общая трудоемкость дисциплины                       | <b>144</b>  | <b>144</b>  |
| <b>Контактная работа, в т.ч. аудиторные занятия</b> | <b>76,6</b> | <b>76,6</b> |
| Лекции  | 30          | 30          |
| <i>в том числе в форме практической подготовки</i>  | –           | –           |
| Лабораторные работы (ЛР)                            | 15          | 15          |
| <i>в том числе в форме практической подготовки</i>  | 15          | 15          |
| Практические занятия (ПЗ)                           | 30          | 30          |
| <i>в том числе в форме практической подготовки</i>  | 30          | 30          |
| Консультации текущие                                | 1,5         | 1,5         |
| <b>Вид аттестации – зачет</b>                       | 0,1         | 0,1         |
| <b>Самостоятельная работа</b>                       | <b>67,4</b> | <b>67,4</b> |
| Подготовка доклада с презентацией                   | 20          | 20          |
| Домашнее задание № 1                                | 24          | 24          |
| Домашнее задание № 2                                | 23,4        | 23,4        |

### 5 Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

#### 5.1 Содержание разделов дисциплины

| № п/п | Наименование разделов дисциплины                   | Содержание раздела  | Трудоемкость раздела, час |
|-------|--|---|---------------------------|
| 1     | Теоретические основы построения защищенных автома- | Системный подход к построению защищенных автоматизированных систем. Понятие сложной системы. Управление и информация, самоорганиза- | 25                        |

|   |  |   |      |
|---|--|---|------|
|   | тизированных систем  | ция. Основные принципы системного подхода при создании сложных систем; Понятие качества и эффективности. Методические вопросы оценки эффективности сложных систем. Функциональная и обеспечивающая часть сложной системы. Технология функционирования сложной системы.  |      |
| 2 | Угрозы безопасности автоматизированных систем                        | Угрозы безопасности локальных и распределённых автоматизированных систем. Проектирование автоматизированных систем. Цели и задачи проектирования. Структуризация предметной области. Классификация объектов проектирования. Жизненный цикл автоматизированной системы. Этапы проектирования системы. Организация работ, функции заказчиков и разработчиков.   | 30   |
| 3 | Проектирование защищённых автоматизированных систем                  | Проектирование и построение системы защиты автоматизированных систем. Практические методы реализации моделей безопасности. Ядра безопасности. Мониторинг взаимодействий в системе. Архитектура защищённых систем. Принципы построения защищённых информационных систем. Технологический цикл реализации защищённой системы обработки и хранения информации. Реализация систем контроля доступа; способы представления информации о правах доступа.                          | 44   |
| 4 | Методы обеспечения безопасности защищённых автоматизированных систем | Методология оценки защищённости изделий и продуктов информационных технологий. Критерии оценки безопасности информационных технологий. Контекст безопасности. Профиль защиты и задание по безопасности. Функциональные требования безопасности. Функциональные классы, семейства и компоненты безопасности. Требования доверия к безопасности. Классы, семейства и компоненты доверия. Оценочный уровень доверия. Критерии оценки профиля защиты и задания по безопасности. | 43,4 |

## 5.2 Разделы дисциплины и виды занятий

| № п/п | Наименование раздела дисциплины                                      | Лекции, час | ЛР, час | ПЗ, час | СР, час |
|-------|--|-------------|---------|---------|---------|
| 1     | Теоретические основы построения защищённых автоматизированных систем | 6           | 3       | 6       | 10      |
| 2     | Угрозы безопасности автоматизированных систем                        | 8           | 4       | 8       | 10      |
| 3     | Проектирование защищённых автоматизированных систем                  | 8           | 4       | 8       | 24      |
| 4     | Методы обеспечения безопасности защищённых автоматизированных систем | 8           | 4       | 8       | 23,4    |

### 5.2.1 Лекции

| № п/п | Наименование раздела дисциплины                                      | Тематика лекционных занятий  | Трудоемкость, Час |
|-------|--|--|-------------------|
| 1     | Теоретические основы построения защищённых автоматизированных систем | Системный подход к построению защищённых автоматизированных систем. Понятие сложной системы. Управление и информация, самоорганизация. Основные принципы системного подхода при создании сложных систем; Понятие качества и эффективности. Методические вопросы оценки эффективности сложных систем. Функциональная и обеспечивающая часть сложной системы. Технология функционирования сложной системы. | 6                 |

|   |  |   |   |
|---|--|---|---|
| 2 | Угрозы безопасности автоматизированных систем                        | Угрозы безопасности локальных и распределённых автоматизированных систем. Проектирование автоматизированных систем. Цели и задачи проектирования. Структуризация предметной области. Классификация объектов проектирования. Жизненный цикл автоматизированной системы. Этапы проектирования системы. Организация работ, функции заказчиков и разработчиков.   | 8 |
| 3 | Проектирование защищённых автоматизированных систем                  | Проектирование и построение системы защиты автоматизированных систем. Практические методы реализации моделей безопасности. Ядра безопасности. Мониторинг взаимодействий в системе. Архитектура защищённых систем. Принципы построения защищённых информационных систем. Технологический цикл реализации защищённой системы обработки и хранения информации. Реализация систем контроля доступа; способы представления информации о правах доступа.                          | 8 |
| 4 | Методы обеспечения безопасности защищённых автоматизированных систем | Методология оценки защищённости изделий и продуктов информационных технологий. Критерии оценки безопасности информационных технологий. Контекст безопасности. Профиль защиты и задание по безопасности. Функциональные требования безопасности. Функциональные классы, семейства и компоненты безопасности. Требования доверия к безопасности. Классы, семейства и компоненты доверия. Оценочный уровень доверия. Критерии оценки профиля защиты и задания по безопасности. | 8 |

### 5.2.2 Практические занятия

| № п/п | Наименование раздела дисциплины                                      | Тематика практических занятий  | Трудоемкость, час |
|-------|--|--|-------------------|
| 1     | Теоретические основы построения защищённых автоматизированных систем | Практическая работа № 1. Проектирование моделей данных с помощью CASE-системы ERWIN для построения защищённых АС   | 6                 |
| 2     | Угрозы безопасности автоматизированных систем                        | Практическая работа № 2. Безопасность в системах с распределёнными базами данных<br>Практическая работа № 3. Организация защищённых соединений при удалённом доступе.  | 8                 |
| 3     | Проектирование защищённых автоматизированных систем                  | Практическая работа № 4. Защита информационных воздействий по протоколу IPSec при использовании Windows 2003 Server.<br>Практическая работа № 5. Обеспечение аутентичности удалённых пользователей посредством применения протоколов CHAP и EAP при организации модемных соединений. | 8                 |
| 4     | Методы обеспечения безопасности защищённых автоматизированных систем | Практическая работа № 6. Настройка клиент-серверного взаимодействия по протоколу защиты данных.<br>Практическая работа № 7. Установка центра сертификации, генерация и отзыв сертификатов в операционной системе Windows   | 8                 |

### 5.2.3 Лабораторный практикум

| № п/п | Наименование раздела дисциплины                                      | Тематика лабораторных занятий  | Трудоемкость, час |
|-------|--|--|-------------------|
| 1     | Теоретические основы построения защищённых автоматизированных систем | Лабораторная работа №1. Создание моделей основных видов АС в защищённом исполнении | 3                 |

|   |  |  |   |
|---|--|--|---|
| 2 | Угрозы безопасности автоматизированных систем                        | Лабораторная работа № 2. Разработка модели угроз и нарушителя для организации                    | 4 |
| 3 | Проектирование защищенных автоматизированных систем                  | Лабораторная работа № 3. Проектирование системы защиты персональных данных для основных видов АС | 4 |
| 4 | Методы обеспечения безопасности защищенных автоматизированных систем | Лабораторная работа № 4. Проектирование АС в защищенном исполнении на примере ИСПДн 1 класса     | 4 |

#### 5.2.4 Самостоятельная работа обучающихся (СРО)

| № п/п | Наименование раздела дисциплины                                      | Вид СРО  | Трудоемкость, час |
|-------|--|--|-------------------|
| 1     | Теоретические основы построения защищенных автоматизированных систем | Подготовка доклада с визуальным представлением средствами PowerPoint | 10                |
| 2     | Угрозы безопасности автоматизированных систем                        |  | 10                |
| 3     | Проектирование защищенных автоматизированных систем                  | Домашнее задание № 1   | 24                |
| 4     | Методы обеспечения безопасности защищенных автоматизированных систем | Домашнее задание № 2   | 23,4              |

### 6 Учебно-методическое и информационное обеспечение дисциплины (модуля)

#### 6.1. Основная литература

1. Давидюк, Н. В. Разработка автоматизированных систем обработки информации в защищенном исполнении : учебное пособие / Н. В. Давидюк. – Санкт-Петербург : Интермедия, 2020. – 48 с. – ISBN 978-5-4383-0194-3. – Текст : электронный // Лань : электронно-библиотечная система. – URL: <https://e.lanbook.com/book/161365>

2. Бабушкин, В. М. Разработка защищенных программных средств информатизации производственных процессов предприятия : учебное пособие / В. М. Бабушкин. – Казань : КНИТУ-КАИ, 2020. – 256 с. – ISBN 978-5-7579-2463-2. – Текст : электронный // Лань : электронно-библиотечная система. – URL: <https://e.lanbook.com/book/193486>

3. Тугов, В. В. Проектирование автоматизированных систем управления : учебное пособие для вузов / В. В. Тугов, А. И. Сергеев, Н. С. Шаров. – 3-е изд., стер. – Санкт-Петербург : Лань, 2022. – 172 с. – ISBN 978-5-8114-8987-9. – Текст : электронный // Лань : электронно-библиотечная система. – URL: <https://e.lanbook.com/book/186064>

4. Потехин, Д. С. Разработка программно-аппаратного обеспечения информационных и автоматизированных систем : учебное пособие / Д. С. Потехин, И. Е. Тарасов. – Москва : РТУ МИРЭА, 2022. – 131 с. – Текст : электронный // Лань : электронно-библиотечная система. – URL: <https://e.lanbook.com/book/240098>

#### 6.2. Дополнительная литература

1. Пономаренко, Д. А. Основы проектирования автоматизированных систем : учебное пособие / Д. А. Пономаренко, Н. И. Безгачин. – 2-е изд., испр. и доп. – Мурманск : МГТУ, 2016. – 154 с. – ISBN 978-5-86185-889-2. – Текст : электронный // Лань : электронно-библиотечная система. – URL: <https://e.lanbook.com/book/142630>

2. Гвоздева, Т. В. Проектирование информационных систем. Стандартиза-

ция, техническое документирование информационных систем : учебное пособие для спо / Т. В. Гвоздева, Б. А. Баллод. – 2-е изд., стер. – Санкт-Петербург : Лань, 2021. – 216 с. – ISBN 978-5-8114-8414-0. – Текст : электронный // Лань : электронно-библиотечная система. – URL: <https://e.lanbook.com/book/176672>

3. Гвоздева, Т. В. Проектирование информационных систем: технология автоматизированного проектирования. Лабораторный практикум : учебное пособие / Т. В. Гвоздева, Б. А. Баллод. – 2-е изд., стер. – Санкт-Петербург : Лань, 2020. – 156 с. – ISBN 978-5-8114-5147-0. – Текст : электронный // Лань : электронно-библиотечная система. – URL: <https://e.lanbook.com/book/133477>

4. Лукьянец, О. Ф. Формализация технологических знаний при разработке автоматизированных систем : учебное пособие / О. Ф. Лукьянец, С. Е. Каминский, О. М. Деев. – Москва : МГТУ им. Н.Э. Баумана, 2014. – 136 с. – ISBN 978-5-7038-3771-9. – Текст : электронный // Лань : электронно-библиотечная система. – URL: <https://e.lanbook.com/book/58416>

### **6.3 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся**

1. Разработка и эксплуатация защищенных автоматизированных систем [Электронный ресурс]: методические указания для самостоятельной работы для студентов, обучающихся по направлению 10.05.03 «Информационная безопасность автоматизированных систем», очной формы обучения / А. В. Скрыпников, Е. В. Чернышова ; ВГУИТ, Кафедра информационной безопасности. - Воронеж : ВГУИТ, 2016. - 20 с. <http://biblos.vsu.ru/ProtectedView/Book/ViewBook/1731>

2. Методические указания для обучающихся по освоению дисциплин (модулей) в ФГБОУ ВО ВГУИТ [Электронный ресурс] : методические указания для обучающихся на всех уровнях высшего образования / М. М. Данылиев, Р. Н. Плотникова; ВГУИТ, Учебно-методическое управление. - Воронеж : ВГУИТ, 2016. – Режим доступа : <http://biblos.vsu.ru/MegaPro/Web/SearchResult/MarcFormat/100813>

### **6.3 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся**

Разработка и эксплуатация защищенных автоматизированных систем [Электронный ресурс]: методические указания для самостоятельной работы для студентов, обучающихся по направлению 10.05.03 – «Информационная безопасность автоматизированных систем», очной формы обучения / А. В. Скрыпников, Е. В. Чернышова ; ВГУИТ, Кафедра информационной безопасности. Воронеж : ВГУИТ, 2016. 20 с. <http://biblos.vsu.ru/ProtectedView/Book/ViewBook/1731>

### **6.4 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины**

| Наименование ресурса сети «Интернет»                                    | Электронный адрес ресурса   |
|---|---|
| «Российское образование» федеральный портал                             | <a href="https://www.edu.ru/">https://www.edu.ru/</a>                           |
| Научная электронная библиотека  | <a href="https://elibrary.ru/defaultx.asp">https://elibrary.ru/defaultx.asp</a> |
| Национальная исследовательская компьютерная сеть России                 | <a href="https://niks.su/">https://niks.su/</a>                                 |
| Информационная система «Единое окно доступа к образовательным ресурсам» | <a href="http://window.edu.ru/">http://window.edu.ru/</a>                       |
| Электронная библиотека ВГУИТ  | <a href="http://biblos.vsu.ru/megapro/web">http://biblos.vsu.ru/megapro/web</a> |
| Сайт Министерства науки и высшего образования РФ                        | <a href="https://minobrnauki.gov.ru/">https://minobrnauki.gov.ru/</a>           |
| Портал открытого on-line образования                                    | <a href="https://npoed.ru/">https://npoed.ru/</a>                               |

## 6.5 Методические указания для обучающихся по освоению дисциплины

Методические указания для обучающихся по освоению дисциплин (модулей) в ФГБОУ ВО ВГУИТ [Электронный ресурс] : методические указания для обучающихся на всех уровнях высшего образования / М. М. Данылиев, Р. Н. Плотникова; ВГУИТ, Учебно-методическое управление. Воронеж : ВГУИТ, 2016. – Режим доступа : <http://biblos.vsu.ru/MegaPro/Web/SearchResult/MarcFormat/100813>. Загл. с экрана

## 6.6 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине , включая перечень программного обеспечения и информационных справочных систем

Microsoft Office профессиональный выпуск версии 2010. Программный пакет «Crypton LITE» («КРИПТОН Шифрование v1.1», «КРИПТОН Подпись v1.1»); Windows 2003 Server; Межсетевой экран; Программный комплекс «КриптоПро АРМ»

Блок управления комплекса радиоконтроля и поиска радиопередающих устройств «ОМЕГА» (переносной), МУ защиты ресурсов сети от внутренних и внешних атак CISCO ASA5505-KB, переносной комплекс для автоматизации измерений при проведении исследований и контроля технических средств ЭВТ «НАВИГАТОР-ПЗГ»; средство активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок «СОНАТА-РЗ.1»; система защиты речевой информации «Соната-АВ-4Б» (Центральный блок питания и управления + Размыкатели в составе СВАЗ Соната АВ); профессиональный обнаружитель скрытых видеокамер СОКОЛ-М (переносной); портативный обнаружитель закладок Protect1203 (переносной); устройство активной защиты информации «ВЕТО-М»; электронный замок Samsung SHS-2920. Страж NT вер.3.0 Сертификат ФСТЭК № 2145 30.07.2013 г.; Ревизор 1XP Сертификат ФСТЭК № 989 08.02.2015 г.; Ревизор 2XP Сертификат ФСТЭК № 990 08.02.2015 г.; Фикс 2.0.2 Сертификат ФСТЭК №1548 15.01.2015 г.; Ревизор сети вер.3.0 Сертификат ФСТЭК №3413 02.06.2015 г.; СЗИ Панцирь К Сертификат ФСТЭК №1973 09.12.2015 г.; СЗИ Dallas Lock 8.0 К Сертификат ФСТЭК №2720 25.09.2015; СЗИ Dallas Lock 8.0 С Сертификат ФСТЭК №2945 16.08.2013.

## 7 Материально-техническое обеспечение дисциплины

|  |   |  |
|--|---|--|
| Лекционные аудитории, оснащенные мультимедийной техникой | Аудио-визуальная система лекционных аудиторий (мультимедийный проектор, экран, усилитель мощности звука, акустические системы, микрофоны, устройство коммутации, сетевой коммутатор для подключения к компьютерной сети (Интернет)) |  |
| Аудитории для проведения лабораторных занятий            | Ауд. 332а: Комплекты мебели для учебного процесса. ПЭВМ – 12 (компьютер Core i5-4570), стенды – 5 шт. Ауд. 424: Комплекты мебели для учебного процесса. ПЭВМ – 12: рабочая  | Ауд.332а:<br>ОС Alt Linux (Альт Образование 8.2) Geany. Lazarus. Qt Creator. Quanta Plus. Вебредактор Bluefish. Среда разработки Code::Blocks. Офисный пакет Libre Office 5.4: Base, Calc, Draw, Impress, Math, Writer. Персональная бухгалтерия HomeBank. |



|  |   |   |
|--|---|---|
|  | <p>станция Регард РДЦБ.;<br/>стенды<br/>– 3<br/>Ауд. 420: Комплекты мебели для учебного процесса. ПЭВМ-11 (компьютер Core i5-4460), проектор Acer projector X1383WH, экран, стенды – 5 шт., блок управления комплекса радиоконтроля и поиска радиопередающих устройств «ОМЕГА» (переносной), МУ защиты ресурсов сети от внутренних и внешних атак CISCO ASA5505-KB, переносной комплекс для автоматизации измерений при проведении исследований и контроля технических средств ЭВТ «НАВИГАТОР-ПЗГ»; средство активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок «СОНАТА-РЗ.1»; система защиты речевой информации «Соната-АВ-4Б» (Центральный блок питания и управления + Размыкатели в составе СВАЗ Соната АВ); профессиональный обнаружитель скрытых видеокамер СОКОЛ-М (переносной); портативный обнаружитель закладок Protect1203 (переносной); устройство активной защиты информации «ВЕТО-М»; электронный замок Samsung SHS-2920</p> | <p>Словарь Star Dict. iTest. VM Maxima. Кумир. Avidemux. Audacios. Brasero. Cheese. SMPlayer. Медиаплеер Parole. Редактор тегов Easy TAG. Stath Studio. Pinta. Веб-браузер Mozilla Firefox. Графический редактор. FP – free Pascal.<br/>Ауд.424:<br/>ОС Alt Linux (Альт Образование 8.2) Geany. Lazarus. Qt Creator. Quanta Plus. Вебредактор Bluefish. Среда разработки Code::Blocks. Офисный пакет Libre Office 5.4: Base, Calc, Draw, Impress, Math, Writer. Персональная бухгалтерия HomeBank. Словарь Star Dict. iTest. VM Maxima. Кумир. Avidemux. Audacios. Brasero. Cheese. SMPlayer. Медиаплеер Parole. Редактор тегов Easy TAG. Stath Studio. Pinta. Веб-браузер Mozilla Firefox. Графический редактор. FP – free Pascal.<br/>Ауд.420:<br/>Microsoft Windows 7 (64 разрядная) Microsoft Office (standart) 2007; Microsoft Access 2007; Microsoft Project 2007; Microsoft Share Point 2007; Microsoft Visio 2007; Microsoft SQL server 2008; 1 С Предприятие Лицензия; 7-Zip File Manager (архиватор); Adobe Acrobat Reader; Adobe Flash Player; FAR file manager; Google Chrome; Java TM 7 (64-bit); KLite Codec Pack; Mozilla Firefox; Oracle VM VirtualBox; Sublime Text; Symantec End-point Protection 12 (Заменен на AVP Kaspersky); VMWare Player; Антивирус “Зоркий глаз”; Lazarus; SmathStudio; NanoCAD; Gimp (графический редактор, аналог Photoshop); Avidemux (видео редактор); Virtual Dub (видео редактор); Free Pascal; Страж NT вер.3.0 Сертификат ФСТЭК № 2145 30.07.2013 г.; Ревизор 1XP Сертификат ФСТЭК № 989 08.02.2015 г.; Ревизор 2XP Сертификат ФСТЭК № 990 08.02.2015 г.; Фикс 2.0.2 Сертификат ФСТЭК №1548 15.01.2015 г.; Ревизор сети вер.3.0 Сертификат ФСТЭК №3413 02.06.2015 г.; СЗИ Панцирь К Сертификат ФСТЭК №1973 09.12.2015 г.; СЗИ Dallas Lock 8.0 К Сертификат ФСТЭК №2720 25.09.2015; СЗИ Dallas Lock 8.0</p> |
| <p>Аудитория для самостоятельной работы студентов (Читальные залы библиотеки)</p>                            | <p>Компьютеры со свободным доступом в сеть Интернет и Электронным библиотечным и информационносправочным системам</p>   |   |
| <p>Аудитория для групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации -</p> | <p>Комплекты мебели для учебного процесса – 30 шт., доска</p>   |   |
| <p>Аудитории для проведения занятий семинарского типа</p>  | <p>Ауд. №332а: комп. класс каф. ИнфБ, количество ПЭВМ-12 (компьютер Cjrei5-4570, ауд.№ 420: комп.</p>   | <p>ОС Alt Linux (Альт Образование 8.2) Geany. Lazarus. Qt Creator. Quanta Plus. Веб-редактор Bluefish. Среда разработки Code::Blocks. Офисный пакет Libre Office 5.4: Base, Calc,</p>   |

|  |  |  |
|--|--|--|
|  | класс каф.ИнфБ, количество ПЭВМ 12,(рабочая станция CPUCore 2DuoE6300 – 1.86), ауд. №424, комп класс каф. ИнфБ, количество ПЭВМ 12 (Компьютер Celeron D 2.8) | Draw, Impress, Math, Writer. Персональная бухгалтерия HomeBank. Словарь Star Dict. iTest. VM Maxima. Кумир. Avidemux. Audacios. Brasero. Cheese. SMPlayer. Медиаплеер Parole. Редактор тегов Easy TAG. Stath Studio. Pinta. Веб-браузер Mozilla Firefox. Графический редактор. FP – free Pascal. |
|--|--|--|

## 8 Оценочные материалы для промежуточной аттестации обучающихся по дисциплине

### 8.1 Оценочные материалы (ОМ) для дисциплины включают:

перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы;

описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания;

типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы;

методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

8.2 Для каждого результата обучения по дисциплине определяются показатели и критерии оценивания сформированности компетенций на различных этапах их формирования, шкалы и процедуры оценивания.

ОМ представляются отдельным комплектом и **входят в состав рабочей программы дисциплины.**

Оценочные материалы формируются в соответствии с П ВГУИТ «Положение об оценочных материалах».

Документ составлен в соответствии с требованиями ФГОС ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем и специализации Безопасность открытых информационных систем.

# **ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ**

— по дисциплине

— Разработка и эксплуатация защищенных автоматизированных систем  
(наименование дисциплины, практики в соответствии с учебным планом)

---

## 1 Перечень компетенций с указанием этапов их формирования

| №п/п | Код компетенции | Содержание компетенции (результат освоения)  | В результате изучения учебной дисциплины обучающийся должен:  |  |   |
|------|-----------------|--|---|--|---|
|      |                 |  | знать   | уметь  | владеть   |
| 1    | ОПК-6           | способностью применять нормативные правовые акты в профессиональной деятельности   | основы документооборота и основные нормативные правовые акты в области информационной безопасности, основные положения ФСТЭК РФ                     | использовать методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных | навыками организации и использования при проведении работ по обеспечению безопасности персональных данных в автоматизированных информационных системах        |
| 2    | ПК-15           | способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем      | основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические) | восстанавливать работоспособность подсистемы информационной безопасности автоматизированных систем в нештатных ситуациях                           | владеть навыками работы с современными инструментальными средствами для исследования программного обеспечения защищенных автоматизированных систем управления |
| 3    | ПК-20           | способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности | основы комплексного обеспечения информационной безопасности распределенных автоматизированных, информационно-управляющих систем                     | решать практические задачи информационной безопасности на основе инфраструктуры открытых ключей  | навыками развертывания и обеспечения работы программных комплексов, обеспечивающих работу с цифровыми сертификатами   |

## 2. Паспорт фонда оценочных средств по дисциплине

| № п/п | Контролируемые модули/разделы/темы дисциплины                 | Индекс контролируемой компетенции (или ее части) | Оценочные средства | Технология оценки (способ контроля) |
|-------|---|--|--------------------|-------------------------------------|
| 1     | Теоретические основы построения защищенных автоматизированных | ОПК-6  | Экзамен            | Проверка преподавателем             |

|   |  |       |   |                         |
|---|--|-------|---|-------------------------|
|   | систем   |       | Кейс-задания к практическим работам                           | Проверка преподавателем |
|   |  |       | Контрольные вопросы к текущим опросам на лабораторных работах | Проверка преподавателем |
|   |  |       | Доклад  | Проверка преподавателем |
| 2 | Угрозы безопасности автоматизированных систем                        | ОПК-6 | Экзамен   | Проверка преподавателем |
|   |  |       | Кейс-задания к практическим работам                           | Проверка преподавателем |
|   |  |       | Доклад  | Проверка преподавателем |
|   |  |       | Контрольные вопросы к текущим опросам на лабораторных работах | Проверка преподавателем |
| 3 | Проектирование защищенных автоматизированных систем                  | ПК-15 | Экзамен   | Проверка преподавателем |
|   |  |       | Кейс-задания к практическим работам                           | Проверка преподавателем |
|   |  |       | Контрольные вопросы к текущим опросам на лабораторных работах | Проверка преподавателем |
|   |  |       | ДЗ № 1  | Проверка преподавателем |
| 4 | Методы обеспечения безопасности защищенных автоматизированных систем | ПК-20 | Экзамен   | Проверка преподавателем |
|   |  |       | Кейс-задания к практическим работам                           | Проверка преподавателем |
|   |  |       | Контрольные вопросы к текущим опросам на лабораторных работах | Проверка преподавателем |
|   |  |       | ДЗ № 2  | Проверка преподавателем |

### 3. Оценочные средства для промежуточной аттестации

#### 3.1 Вопросы к собеседованию на экзамене

3.1.1. ОПК-6 - способностью применять нормативные правовые акты в профессиональной деятельности

| № задания | Формулировка вопроса  |
|-----------|---|
| 1         | История развития, назначение и роль автоматизированных систем.                                    |
| 2         | Этапы развития информационных систем.   |
| 3         | Классификация автоматизированных систем.  |
| 4         | Основные понятия и определения теории сложных систем.   |
| 5         | Классификация систем. Функциональная и обеспечивающая часть сложной системы.                      |
| 6         | Основные требования и принципы построения систем защиты информации в автоматизированных системах. |
| 7         | Архитектура построения защищенных автоматизированных систем.                                      |
| 8         | Основные положения современной концепции информационной безопасности автоматизированных систем.   |
| 9         | Методология построения и функционирования систем безопасности информации в АС.                    |
| 10        | Пути практической реализации концепции комплексной защиты информации в АС.                        |

3.1.2. ПК-15 - способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем

|    |  |
|----|--|
| 11 | Понятие качества и эффективности сложных систем. |
|----|--|

|    |  |
|----|--|
| 12 | Характеристики качества.   |
| 13 | Определение и содержание понятия угрозы безопасности автоматизированных систем.            |
| 14 | Классификация угроз безопасности АС.   |
| 15 | Цели и задачи оценки угроз безопасности АС. Методы и модели анализа угроз безопасности АС. |
| 16 | Цели и задачи проектирования АС.   |
| 17 | Классификация объектов проектирования.   |

3.1.3. ПК-20 - способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности

|    |   |
|----|---|
| 18 | Состояние проблемы защиты информации в АС.  |
| 19 | Принципы и условия, способствующие повышению эффективности защиты информации в АС.    |
| 20 | Общие требования к системам защиты информации в АС.                                   |
| 21 | Характеристика и принципы построения систем защиты информации в АС.                   |
| 22 | Методика выбора средств и организация защиты информации в АС.                         |
| 23 | Принципы построения и функционирования распределенных автоматизированных систем.      |
| 24 | Основные положения концепции построения и использования распределенных защищенных АС. |
| 25 | Содержание этапов проектирования АС.  |
| 26 | Реальные и мнимые угрозы.   |
| 27 | Показатели и критерии эффективности   |
| 28 | Организация работ, функции заказчиков и разработчиков.                                |

### 3.2 Контрольные вопросы к текущим опросам на лабораторных работах

3.2.1. ОПК-6 - способностью применять нормативные правовые акты в профессиональной деятельности

| № задания | Формулировка вопроса  |
|-----------|---|
| 1.        | Основные средства и способы обеспечения информационной безопасности в автоматизированных Системах |
| 2.        | Принципы построения систем защиты информации  |
| 3.        | Понятие и классификация угроз безопасности автоматизированных систем                              |
| 4.        | Базовая модель угроз безопасности информации  |
| 5.        | Методика оценки угроз безопасности Информации   |

3.2.2. ПК-15 - способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем

|   |  |
|---|--|
| 1 | Последовательность стадий и содержание этапов разработки автоматизированных систем в защищенном исполнении |
| 2 | Содержание этапов проектирования автоматизированных систем в защищенном исполнении                         |
| 3 | Требования по защите сведений о создаваемой АС   |
| 4 | Модели данных, систем и процессов защиты информации в автоматизированных системах                          |

3.2.3. ПК-20 - способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности

|    |  |
|----|--|
| 1. | Технологии автоматизированного проектирования автоматизированных информационных систем                       |
| 2. | Оценка защищенности АС на основе отечественных стандартов и нормативно- методических документов ФСТЭК России |
| 3. | Понятие и архитектура распределенных автоматизированных систем   |
| 4. | Особенности способов и средств защиты информации в распределенных автоматизированных системах                |
| 5. | Состав и содержание организационных и технических мер по защите информационных систем персональных данных    |
| 6. | Порядок обеспечения защиты информации при эксплуатации АС  |
| 7. | Общие обязанности администратора информационной безопасности автоматизированной системы                      |

### 3.3. Темы докладов

### 3.3.1. ОПК-6 - способностью применять нормативные правовые акты в профессиональной деятельности ,

| № задания | Формулировка задания  |
|-----------|---|
| 1.        | ГОСТ Р 50922-2006 — Защита информации. Основные термины и определения.  |
| 2.        | ГОСТ Р ИСО/МЭК 15408-1-2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель                 |
| 3.        | ГОСТ Р ИСО/МЭК 15408-2-2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности. |
| 4.        | ГОСТ Р ИСО/МЭК 15408-3-2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности.      |
| 5.        | ГОСТ Р ИСО/МЭК 15408 — «Общие критерии оценки безопасности информационных технологий»   |
| 6.        | ГОСТ Р ИСО/МЭК 17799 — «Информационные технологии. Практические правила управления информационной безопасностью». Прямое применение международного стандарта с дополнением — ISO/IEC 17799:2005               |
| 7.        | ГОСТ Р ИСО/МЭК 27001 — «Информационные технологии. Методы безопасности. Система управления безопасностью информации. Требования». Прямое применение международного стандарта — ISO/IEC 27001:2005.            |
| 8.        | ГОСТ Р 51898-2002 — Аспекты безопасности. Правила включения в стандарты   |
| 9.        | Защищенная автоматизированная система   |
| 10.       | Модели угроз информационной безопасности  |
| 11.       | Модель нарушителя информационной безопасности   |
| 12.       | Персональные данные. Особенности хранения и передачи  |
| 13.       | Понятие и требования к ИСПДн  |
| 14.       | Практические подходы к разработке моделей нарушителя  |
| 15.       | Понятие персональных данных. Понятие ИСПДн.   |
| 16.       | Федеральное законодательство в области защиты персональных данных и ведомственные нормативные акты (ФСТЭК России, ФСБ России).  |

### 3.4. Домашнее задание № 1

3.4.1. ПК-15 - способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем

| № задания | Формулировка задания  |
|-----------|---|
| 1         | Разработать модель разрешительной системы ролевого управления доступом в автоматизированной системе, с учетом:<br>- групп пользователей (не более 5 ролей);<br>- выполняемых функций группами пользователей;<br>- наименования информационного ресурса;<br>- меток конфиденциальности информационного ресурса;<br>- мест хранения информационного ресурса (каталог HDD);<br>- прав на доступ к информации (R - чтение, W - запись, D - удаление, N - переименование, E - исполнение, M - модификация, A - полный доступ). |

### 3.5. Домашнее задание № 2

3.5.1. ПК-20 - способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности

| № задания | Формулировка задания  |
|-----------|---|
| 1         | Разработать частную модель угроз безопасности распределенной информационной системы персональных данных (ИС ПДн) с подключением к сети международного информационного обмена по следующим исходным данным:<br>- локальная ИС ПДн, развернута в пределах нескольких близко расположенных зданий; |

|  |  |
|--|--|
|  | <ul style="list-style-type: none"> <li>- имеет многоточечный выход в сеть общего пользования;</li> <li>- позволяет запись, удаление, сортировку ПДн;</li> <li>- имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн;</li> <li>- используется одна база ПДн, принадлежащая организации - владельцу данной ИСПДн;</li> <li>- данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации;</li> <li>- предоставляются сторонним пользователям ИС ПДн без предварительной обработки только часть ПДн.</li> </ul> |
|--|--|

### 3.6. Кейс-задания к практическим работам

#### 3.6.1. ОПК-6 - способностью применять нормативные правовые акты в профессиональной деятельности

| № задания | Формулировка задания   |
|-----------|--|
| 1.        | <p>Определить базовый уровень защищенности ИС ПДн по следующим исходным данным:</p> <ul style="list-style-type: none"> <li>- обработка ПДн сотрудников организации;</li> <li>- категории биометрических и иных персональных данных;</li> <li>- объем обработки менее 100000 субъектов персональных данных;</li> <li>- возможны угрозы 2 типа.</li> </ul>   |
| 2.        | <p>Определить состав и содержание организационных и технических мер по защите ИС ПДн в соответствии с уровнем защищенности, руководствуясь последовательностью действий:</p> <ul style="list-style-type: none"> <li>- определить базовый набор мер для третьего уровня защищенности ПДн;</li> <li>- адаптировать базовый набор мер, с учетом характеристик распределенной информационной системы;</li> <li>- подготовить предложения для уточнения адаптированного базового набора мер для различных вариантов ИС ПДн.</li> </ul> <p>Подобрать необходимый для заданного уровня защищенности ПДн состав средств защиты информации.</p> |
| 3         | <p>Разработать структуру технического задания на создание автоматизированной системы в защищенном исполнении. Составить технический паспорт на автоматизированную систему в защищенном исполнении, включающий:</p> <ul style="list-style-type: none"> <li>- общие сведения об автоматизированной системе;</li> <li>- состав оборудования автоматизированной системы (состав основных и вспомогательных средств и систем);</li> <li>- состав средств защиты информации.</li> </ul>  |
| 4         | <p>Разработать перечень сведений конфиденциального характера предприятия, с учетом видов информации ограниченного доступа (коммерческая тайна, персональные данные), и требуемых этапов разработки подобного перечня. Для сформированного перечня определить состав объектов защиты</p>  |

#### 3.6.2. ПК-15 - способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем

|    |  |
|----|--|
| 1. | <p>Разработать модель системы (элемента системы) защиты информации, используя один из методов:</p> <ul style="list-style-type: none"> <li>- специальные методы неформального моделирования.</li> <li>- декомпозицию общей задачи на частные задачи.</li> <li>- прием макро моделирования</li> </ul>  |
| 2. | <p>Разработать основные положения Методики анализа и оценки рисков информационной безопасности в соответствии с выбранной областью действия системы управления информационной безопасностью и активами. В содержание Методики анализа и оценки рисков информационной безопасности включить:</p> <ul style="list-style-type: none"> <li>- порядок инвентаризации активов;</li> <li>- порядок оценки ценности активов, шкалы оценки ценности;</li> <li>- порядок определения угроз и уязвимостей активов, определения вероятности их возникновения;</li> <li>- порядок оценки рисков информационной безопасности;</li> </ul> |



|    |  |
|----|--|
|    | - порядок формирования мер по обработке рисков.  |
| 3. | Разработать программу проведения аудита первой стороны, включающую:<br>- внутренние требования системы управления информационной безопасностью;<br>- состав проверяемых подразделений;<br>- вид аудиторской проверки;<br>- метрики оценки эффективности аудита |

3.6.3. ПК-20 - способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности

|   |  |
|---|--|
| 1 | Разработать модель реализации преднамеренного инцидента информационной безопасности, с учетом:<br>- перечня злоумышленников;<br>- целей злоумышленников;<br>- методов и средств реализации информационного воздействия;<br>- действий злоумышленников;<br>- объектов информационного воздействия;<br>- результатов информационного воздействия |
| 2 | Найти ключевые точки сообщения с окружающим программно-аппаратным обеспечением (адреса памяти, файлы на диске, сетевые ресурсы) сервиса, используя средства мониторинга активности приложения. Предложить список мер по программной защите приложения от внешних атак на данные точки сообщения  |
| 3 | Используя средства агрессивного сканирования портов, симитировать атаку на распределенную информационную систему в кабинете. Оценить успешность атаки, построить оценку защищенности сети по полученным данным.  |
| 4 | На основе заданной схемы незащищенной корпоративной ЛВС предприятия разработать схему защищенной сети с использованием следующих средств активной защиты: фаерволл, интерактивный детектор атак. Привести конфигурацию фаерволла для заданного перечня сервисов.   |

**4. Методические материалы,  
определяющие процедуры оценивания знаний, умений, навыков  
и (или) опыта деятельности,  
характеризующих этапы формирования компетенций**

Процедуры оценивания в ходе изучения дисциплины знаний, умений и навыков, характеризующих этапы формирования компетенций, регламентируются положениями:

- П ВГУИТ 2.4.03 – 2015 Положение о курсовых, экзаменах и зачетах;
- П ВГУИТ 4.1.02 – 2012 Положение о рейтинговой оценке текущей успеваемости.

Итоговая оценка по дисциплине определяется на основании определения средневзвешенному значения баллов по каждому заданию.

### 5. Описание показателей и критериев оценивания уровня сформированности компетенций

| Результаты обучения по этапам формирования компетенций   | Методика оценки (объект, продукт или процесс)                 | Показатель оценивания       | Критерии оценивания сформированности компетенций   | Шкала оценивания               |                              |
|--|---|-----------------------------|--|--------------------------------|------------------------------|
|  |   |                             |  | Академическая оценка или баллы | Уровень освоения компетенции |
| ОПК-6 - способностью применять нормативные правовые акты в профессиональной деятельности   |   |                             |  |                                |                              |
| ЗНАТЬ:<br>основы документооборота и основные нормативные правовые акты в области информационной безопасности, основные положения ФСТЭК РФ                    | Экзамен   | Уровень владения материалом | ответил на все вопросы, допустил не более 1 ошибки в ответе  | Отлично                        | Освоена (повышенный)         |
|  |   |                             | ответил на все вопросы, допустил более 1, но менее 3 ошибок  | Хорошо                         | Освоена (повышенный)         |
|  |   |                             | ответил не на все вопросы, но в тех, на которые дал ответ не допустил ошибки   | Удовлетворительно              | Освоена (базовый)            |
|  |   |                             | ответил не на все вопросы, допустил более 5 ошибок   | Неудовлетворительно            | Не освоена (недостаточный)   |
| УМЕТЬ:<br>использовать методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных | Контрольные вопросы к текущим опросам по лабораторным работам | Уровень умения              | студент выполнил задание и ответил на все вопросы и допустил не более 1 ошибки в ответе                              | Отлично                        | Освоена (повышенный)         |
|  |   |                             | студент выполнил задание и ответил на все вопросы и допустил более 1 ошибки, но менее 3 ошибок                       | Хорошо                         | Освоена (повышенный)         |
|  |   |                             | студент выполнил задание не полностью и ответил не на все вопросы, но в тех, на которые дал ответ не допустил ошибки | Удовлетворительно              | Освоена (базовый)            |
|  |   |                             | студент ответил не на все вопросы, допустил более 5 ошибок   | Неудовлетворительно            | Не освоена (недостаточный)   |
|  | Кейс-задания к практическим работам                           | Уровень умения              | студент выполнил задание и ответил на все вопросы и допустил не более 1 ошибки в ответе                              | Отлично                        | Освоена (повышенный)         |
|  |   |                             | студент выполнил задание и ответил на все вопросы и допустил более 1 ошибки, но менее 3 ошибок                       | Хорошо                         | Освоена (повышенный)         |
|  |   |                             | студент выполнил задание не полностью и ответил не на все вопросы, но в тех, на которые дал ответ                    | Удовлетворительно              | Освоена (базовый)            |

|  |   |                             |   |                                |                               |
|--|---|-----------------------------|---|--------------------------------|-------------------------------|
|  |   |                             | не допустил ошибки  |                                |                               |
|  |   |                             | студент ответил не на все вопросы, допустил более 5 ошибок  | Неудовлетворительно            | Не освоена (недостаточный)    |
| ВЛАДЕТЬ:<br>навыками организации и использования при проведении работ по обеспечению безопасности персональных данных в автоматизированных информационных системах | Доклад  | Уровень владения            | выставляется студенту при наличии доклада, преобразовании информации в единую форму, т.е. презентации по выбранной теме   | Зачтено                        | Освоена (повышенный, базовый) |
|  |   |                             | выставляется студенту при наличии информации только из одного источника, и (или) отсутствии презентации по выбранной теме | Не зачтено                     | Не освоена (недостаточный)    |
|  |   |                             |   | Академическая оценка или баллы | Уровень освоения компетенции  |
| ПК-15 - способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем        |   |                             |   |                                |                               |
| ЗНАТЬ:<br>основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические)      | Экзамен   | Уровень владения материалом | ответил на все вопросы, допустил не более 1 ошибки в ответе   | Отлично                        | Освоена (повышенный)          |
|  |   |                             | ответил на все вопросы, допустил более 1, но менее 3 ошибок   | Хорошо                         | Освоена (повышенный)          |
|  |   |                             | ответил не на все вопросы, но в тех, на которые дал ответ не допустил ошибки  | Удовлетворительно              | Освоена (базовый)             |
|  |   |                             | ответил не на все вопросы, допустил более 5 ошибок  | Неудовлетворительно            | Не освоена (недостаточный)    |
| УМЕТЬ:<br>восстанавливать работоспособность подсистемы информационной безопасности автоматизированных систем в нестандартных ситуациях                             | Контрольные вопросы к текущим опросам по лабораторным работам | Уровень умения              | студент выполнил задание и ответил на все вопросы и допустил не более 1 ошибки в ответе                                   | Отлично                        | Освоена (повышенный)          |
|  |   |                             | студент выполнил задание и ответил на все вопросы и допустил более 1 ошибки, но менее 3 ошибок                            | Хорошо                         | Освоена (повышенный)          |
|  |   |                             | студент выполнил задание не полностью и ответил не на все вопросы, но в тех, на которые дал ответ не допустил ошибки      | Удовлетворительно              | Освоена (базовый)             |

|   |                                     |                             |   |                     |                               |
|---|-------------------------------------|-----------------------------|---|---------------------|-------------------------------|
|   |                                     |                             | студент ответил не на все вопросы, допустил более 5 ошибок  | Неудовлетворительно | Не освоена (недостаточный)    |
|   | Кейс-задания к практическим работам | Уровень умения              | студент выполнил задание и ответил на все вопросы и допустил не более 1 ошибки в ответе                                   | Отлично             | Освоена (повышенный)          |
|   |                                     |                             | студент выполнил задание и ответил на все вопросы и допустил более 1 ошибки, но менее 3 ошибок                            | Хорошо              | Освоена (повышенный)          |
|   |                                     |                             | студент выполнил задание не полностью и ответил не на все вопросы, но в тех, на которые дал ответ не допустил ошибки      | Удовлетворительно   | Освоена (базовый)             |
|   |                                     |                             | студент ответил не на все вопросы, допустил более 5 ошибок  | Неудовлетворительно | Не освоена (недостаточный)    |
| ВЛАДЕТЬ:<br>владеть навыками работы с современными инструментальными средствами для исследования программного обеспечения защищенных автоматизированных систем управления | Доклад                              | Уровень владения            | выставляется студенту при наличии доклада, преобразовании информации в единую форму, т.е. презентации по выбранной теме   | Зачтено             | Освоена (повышенный, базовый) |
|   |                                     |                             | выставляется студенту при наличии информации только из одного источника, и (или) отсутствии презентации по выбранной теме | Не зачтено          | Не освоена (недостаточный)    |
| ПК-20 - способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности          |                                     |                             |   |                     |                               |
| ЗНАТЬ:<br>основы комплексного обеспечения информационной безопасности распределенных автоматизированных, информационно-управляющих систем                                 | Экзамен                             | Уровень владения материалом | ответил на все вопросы, допустил не более 1 ошибки в ответе   | Отлично             | Освоена (повышенный)          |
|   |                                     |                             | ответил на все вопросы, допустил более 1, но менее 3 ошибок   | Хорошо              | Освоена (повышенный)          |
|   |                                     |                             | ответил не на все вопросы, но в тех, на которые дал ответ не допустил ошибки  | Удовлетворительно   | Освоена (базовый)             |
|   |                                     |                             | ответил не на все вопросы, допустил более 5 ошибок  | Неудовлетворительно | Не освоена (недостаточный)    |
| УМЕТЬ:<br>решать практические задачи информационной безопасности на основе инфраструктуры   | Контрольные вопросы к текущим оп-   | Уровень умения              | студент выполнил задание и ответил на все вопросы и допустил не более 1 ошибки в ответе                                   | Отлично             | Освоена (повышенный)          |

|   |                                     |                 |  |                     |                            |
|---|-------------------------------------|-----------------|--|---------------------|----------------------------|
| открытых ключей   | росам по лабораторным работам       |                 | студент выполнил задание и ответил на все вопросы и допустил более 1 ошибки, но менее 3 ошибок   | Хорошо              | Освоена (повышенный)       |
|   |                                     |                 | студент выполнил задание не полностью и ответил не на все вопросы, но в тех, на которые дал ответ не допустил ошибки   | Удовлетворительно   | Освоена (базовый)          |
|   |                                     |                 | студент ответил не на все вопросы, допустил более 5 ошибок   | Неудовлетворительно | Не освоена (недостаточный) |
|   | Кейс-задания к практическим работам | Уровень умения  | студент выполнил задание и ответил на все вопросы и допустил не более 1 ошибки в ответе  | Отлично             | Освоена (повышенный)       |
|   |                                     |                 | студент выполнил задание и ответил на все вопросы и допустил более 1 ошибки, но менее 3 ошибок   | Хорошо              | Освоена (повышенный)       |
|   |                                     |                 | студент выполнил задание не полностью и ответил не на все вопросы, но в тех, на которые дал ответ не допустил ошибки   | Удовлетворительно   | Освоена (базовый)          |
|   |                                     |                 | студент ответил не на все вопросы, допустил более 5 ошибок   | Неудовлетворительно | Не освоена (недостаточный) |
| ВЛАДЕТЬ:<br>навыками развертывания и обеспечения работы программных комплексов, обеспечивающих работу с цифровыми сертификатами | Домашняя работа № 1                 | Уровень навыков | студент выбрал верную методику решения задач, ответил на все вопросы, допустил не более 1 ошибки в ответе  | Отлично             | Освоена (повышенный)       |
|   |                                     |                 | студент выбрал верную методику решения задач, проведен верный расчет ответил на все вопросы, имеются незначительные замечания по тексту и оформлению работы, допустил не более 3 ошибок в ответе | Хорошо              | Освоена (повышенный)       |
|   |                                     |                 | студент выбрал верную методику решения задач, проведен верный расчет, представил решение задач, ответил на все вопросы, имеются значительные замечания по тексту                                 | Удовлетворительно   | Освоена (базовый)          |

|  |                    |                        |  |                      |                            |
|--|--------------------|------------------------|--|----------------------|----------------------------|
|  |                    |                        | и оформлению работы, допустил не более 5 ошибок в ответе   |                      |                            |
|  |                    |                        | студент выбрал верную методику решения задач, проведен верный расчет, выполнил правильно графическую часть, представил решение задач, ответил на все вопросы, имеются значительные замечания по тексту и оформлению работы, допустил более 5 ошибок в ответе | Не удовлетворительно | Не освоена (недостаточный) |
|  | Домашняя работа №2 | Методика решения задач | студент выбрал верную методику решения задач, ответил на все вопросы, допустил не более 1 ошибки в ответе  | Отлично              | Освоена (повышенный)       |
|  |                    |                        | студент выбрал верную методику решения задач, проведен верный расчет ответил на все вопросы, имеются незначительные замечания по тексту и оформлению работы, допустил не более 3 ошибок в ответе   | Хорошо               | Освоена (повышенный)       |
|  |                    |                        | студент выбрал верную методику решения задач, проведен верный расчет, представил решение задач, ответил на все вопросы, имеются значительные замечания по тексту и оформлению работы, допустил не более 5 ошибок в ответе                                    | Удовлетворительно    | Освоена (базовый)          |
|  |                    |                        | студент выбрал верную методику решения задач, проведен верный расчет, выполнил правильно графическую часть, представил решение задач, ответил на все вопросы, имеются значительные замечания по тексту и оформлению работы, допустил более 5 ошибок в ответе | Не удовлетворительно | Не освоена (недостаточный) |