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

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 00A29CA99D98126F4EB57F6F989D713C88
Владелец: Василенко Виталий Николаевич
Действителен: с 07.07.2022 до 30.09.2023

**УТВЕРЖДАЮ**
Проректор по учебной работе

_____ Василенко В.Н.
(подпись) (Ф.И.О.)

«25» мая 2023

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

## Информационная безопасность открытых 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**

Целями и задачами освоения дисциплины «Информационная безопасность открытых систем» в соответствии с видами профессиональной деятельности являются:

– моделирование и исследование свойств защищенных автоматизированных систем;

– анализ защищенности информации в автоматизированных системах и безопасности реализуемых информационных технологий;

– разработка эффективных решений по обеспечению информационной безопасности автоматизированных систем.

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 | Компетенции | Содержание компетенции (результат освоения) | В результате изучения учебной дисциплины обучающийся должен : | | |
|---|---|---|---|---|---|
| | | | знать | уметь | владеть |
| 1 | ПК -3 | способность проводить анализ защищенности автоматизированных систем. | основные методы и средства реализации удаленных сетевых атак на открытые информационные системы, принцип работы сетевых протоколов и технологий передачи данных в открытых информационных системах. Политики безопасности и меры защиты в открытых информационных системах | применять основные методы и средства реализации удаленных сетевых атак на открытые информационные системы, принципы работы сетевых протоколов и технологий передачи данных в открытых информационных системах, политики безопасности и меры защиты в открытых информационных системах | навыками анализа угроз и уязвимостей в открытых информационных системах, терминологией и системным подходом построения информационных защищенных открытых систем, навыками построения политик безопасности в открытых информационных системах |
| 2 | ОПК-4 | способностью понимать значение информации в развитии современного общества, применять достижения современных информационных | знать и понимать способность значения информации в развитии современного общества, знать достижения современных информационных технологий для по- | применять на практике способность значения информации в развитии современного общества, знать достижения современных информационных технологий для поиска | навыками применения на практике способности значения информации в развитии современного общества, знать достижения современных ин- |

| | | | | | |
|---|---|---|---|---|---|
| | | технологий для поиска информации в компьютерных системах, сетях, библиотечных фондах | иска информации в компьютерных системах, сетях. | информации в компьютерных системах, сетях | формационных технологий для поиска информации в компьютерных системах, сетях |

**3.Место дисциплины в структуре ОП ВО**

Дисциплина (модуль) относится к блоку 1 ОП и ее базовой части.

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

- Информатика;
- Теория информации;
- Технологии разработки защищенного документооборота;
- Безопасность операционных систем;
- Система обнаружения компьютерных атак;
- Открытые информационные системы;
- Учебная практика, ознакомительная;
- Учебная практика, практика по получению первичных профессиональных умений.

Дисциплина является предшествующей для изучения дисциплин, прохождения практик:

- Техническая защита информации;
- Криптографические методы защиты информации;
- Производственная практика, преддипломная практика;
- Производственная практика, практика по получению профессиональных умений и опыта профессиональной деятельности;

защиты выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты.

**4. Объем дисциплины и виды учебных занятий**

Общая трудоемкость дисциплины составляет 5 зачетных единиц.

| **Виды учебной работы** | **Всего часов** | **Семестр** |
|---|---|---|
| | | **6** |
| | **акад.** | **акад.** |
| Общая трудоемкость дисциплины | **180** | **180** |
| **Контактная работа** в т.ч. аудиторные занятия: | **75,1** | **75,1** |
| Лекции | 18 | 18 |
| *в том числе в форме практической подготовки* | – | – |
| Лабораторные работы (ЛР) | 18 | 18 |
| *в том числе в форме практической подготовки* | 18 | 18 |
| Практические занятия (ПЗ) | 36 | 36 |
| *в том числе в форме практической подготовки* | 36 | 36 |
| Консультации текущие | 1,9 | 1,9 |
| Консультация перед экзаменом | 2 | 2 |
| Виды аттестации (экзамен) | 0,2 | 0,2 |
| **Самостоятельная работа** | **71,1** | **71,1** |
| Отчеты по лабораторным и практическим работам | 29 | 29 |
| Подготовка к тестированию | 16 | 16 |
| Домашнее задание | 8 | 8 |
| Расчетно-практическая работа | 18,1 | 18,1 |
| **Подготовка к экзамену (контроль)** | **33,8** | **33,8** |

**5 Содержание дисциплины, 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 | Часов по разделу |
|---|---|---|---|
| 1 | Стандартизация и модельное представление открытых информационных систем | Основные элементы технологии открытых информационных систем. Совместимость открытых систем. Переносимость. Способность К взаимодействию. Основные модели открытых систем. | 14 |
| 2 | Уязвимость открытых систем на примере интернета | Основные понятия. Угрозы ресурсам интернета и причины их реализации. Уязвимость архитектуры клиент-сервер. Слабости системных утилит, команд и сетевых сервисов: Telnet, FTP, NFS, DNS, NIS, World Wide Web, Команды удаленного выполнения, Sendmail и электронная почта. Слабости современных технологий программирования. Ошибки в программном обеспечении сетевые вирусы. | 21 |
| 3 | Атаки на открытые информационные системы | Удаленные атаки на открытые системы. Типичные сценарии и уровни атак. Классические и современные методы, используемые нападающими для проникновения в открытые системы. | 17 |
| 4 | Обеспечение информационной безопасности в открытых системах | Четырехуровневая модель открытой системы. Специфика защиты ресурсов открытых систем на примере интернета. Выбор сетевой топологии интернета при подключении к другим внешним сетям. Принципы создания защищенных средств связи объектов в открытых системах. Политика безопасности для открытых систем. Сервисы безопасности. Средства обеспечения информационной безопасности в открытых системах. Создание комплексной системы обеспечения безопасности открытых систем. | 20 |
| 5 | Аутентификация субъектов и объектов взаимодействия в открытых системах | Сетевая аутентификация – «первый рубеж» защиты открытой системы. Подсистема аутентификации. Российский рынок средств аутентификации. | 18 |
| 6 | Межсетевые экраны | Функции межсетевых экранов. Руководящий документ Гостехкомиссии России по межсетевым экранам. Профили защиты для межсетевых экранов. Типы межсетевых экранов. Основные компоненты межсетевого экрана. Схемы подключения межсетевых экранов. Слабости межсетевых экранов. Выбор реализаций межсетевых экранов. | 18 |
| 7 | Системы анализа защищенности | Аудит и мониторинг информационной безопасности в открытых системах. Место и задачи систем анализа защищенности в защите открытых систем. Классификации систем анализа защищенности. Сетевые сканеры. Сканеры безопасности для приложений. Критерии выбора сканеров безопасности. | 17,1 |
| 8 | Системы обнаружения и предотвращения вторжений | Строения систем обнаружения вторжений. Системное обнаружение вторжений. Сетевое обнаружение вторжений. Поведенческое обнаружение вторжений. Интеллектуальное обнаружение вторжений. Комплексное обнаружение вторжений. Выбор системы обнаружения вторжений | 18 |

## 5.2 Разделы дисциплины и виды занятий

| № п/п | Наименование раздела дисциплины | Лекции, час | ЛР, час | ПЗ, час | СР, час |
|---|---|---|---|---|---|
| 1 | Стандартизация и модельное представление открытых информационных систем | 2 | | 4 | 8 |
| 2 | Уязвимость открытых систем на примере интернета | 2 | 5 | 4 | 10 |
| 3 | Атаки на открытые информационные системы | 3 | | 4 | 10 |
| 4 | Обеспечение информационной безопасности в открытых системах | 2 | 5 | 4 | 9 |
| 5 | Аутентификация субъектов и объектов взаимодействия в открытых системах | 2 | 4 | 4 | 8 |
| 6 | Межсетевые экраны | 2 | 4 | 4 | 8 |
| 7 | Системы анализа защищенности | 3 | | 6 | 8,1 |
| 8 | Системы обнаружения и предотвращения вторжений | 2 | | 6 | 10 |

5.2.1 Лекции

| № п/п | Наименование раздела дисциплины | Тематика лекционных занятий | Трудоемкость , час |
|---|---|---|---|
| 1 | Стандартизация и модельное представление открытых информационных систем | Основные элементы технологии открытых информационных систем. Совместимость открытых систем. Переносимость. Способность к взаимодействию. Основные модели открытых систем. | 2 |
| 2 | Уязвимость открытых систем на примере интернета | Основные понятия. Угрозы ресурсам интернета и причины их реализации. Уязвимость архитектуры клиент-сервер. Слабости системных утилит, команд и сетевых сервисов: Telnet, FTP, NFS, DNS, NIS, World Wide Web, Команды удаленного выполнения, Sendmail и электронная почта. Слабости современных технологий программирования. Ошибки в программном обеспечении. | 3 |
| 3 | Атаки на открытые информационные системы | Удаленные атаки на открытые системы. Типичные сценарии и уровни атак. Классические и современные методы, используемые нападающими для проникновения в открытые системы. | 2 |
| 4 | Обеспечение информационной безопасности в открытых системах | Четырехуровневая модель открытой системы. Специфика защиты ресурсов открытых систем на примере интернета. Выбор сетевой топологии интернета при подключении к другим внешним сетям. Принципы создания защищенных средств связи объектов в открытых системах. Политика безопасности для открытых систем. Сервисы безопасности. Средства обеспечения информационной безопасности в открытых системах. Создание комплексной системы обеспечения безопасности открытых систем. | 2 |
| 5 | Аутентификация субъектов и объектов взаимодействия в открытых системах | Сетевая аутентификация – «первый рубеж» защиты открытой системы. Подсистема аутентификации. Российский рынок средств аутентификации | 2 |
| 6 | Межсетевые экраны | Функции межсетевых экранов. Руководящий документ Гостехкомиссии России по межсетевым экранам. Профили защиты для межсете- | 2 |

| | | | |
|---|---|---|---|
| | | вых экранов. Типы межсетевых экранов. Основные компоненты межсетевого экрана. Схемы подключения межсетевых экранов. Слабости межсетевых экранов. Выбор реализаций межсетевых экранов | |
| 7 | Системы анализа защищенности | Аудит и мониторинг информационной безопасности в открытых системах. Место и задачи систем анализа защищенности в защите открытых систем. Классификации систем анализа защищенности. Сетевые сканеры Сканеры безопасности для приложений. Критерии выбора сканеров безопасности. | 3 |
| 8 | Системы обнаружения и предотвращения вторжений | Методы отражения вторжений. Основы построения систем обнаружения вторжений. Системное обнаружение вторжений. Сетевое обнаружение вторжений. Поведенческое обнаружение вторжений. Интеллектуальное обнаружение вторжений. Комплексное обнаружение вторжений. Выбор системы обнаружения вторжений. | 2 |

### 5.2.2 Практические занятия

| № п/п | Наименование раздела дисциплины | Тематика практических занятий | Трудоемкость, час |
|---|---|---|---|
| 1 | Стандартизация и модельное представление открытых информационных систем | Основные группы стандартов и организации по стандартизации. Модель OSI и POSIX. | 4 |
| 2 | Уязвимость открытых систем на примере интернета | Разработка и управление Политикой использования ресурсов интернета | 4 |
| 3 | Атаки на открытые информационные системы | Атаки на открытые системы: анализ сетевого трафика, подмена доверенного объекта или субъекта, ложный объект, «отказ в обслуживании», удаленный контроль над станцией в сети | 4 |
| 4 | Обеспечение информационной безопасности в открытых системах | Создания защищенных средств связи объектов в открытых системах на основе стандартов ISO 7498-2, 17799, 15408. Слабости системных утилит, команд и сетевых сервисов: Telnet, FTP, NFS, DNS, NIS, World Wide Web, Команды удаленного выполнения, Sendmail и электронная почта | 4 |
| 5 | Аутентификация субъектов и объектов взаимодействия в открытых системах | Построение единых систем аутентификации, авторизации, персонализации, делегированного управления данными о субъектах и объектах и аудита доступа Анализ типовой модели аутентификации | 4 |
| 6 | Межсетевые экраны | Типы межсетевых экранов: экранирующие концентраторы, пакетные фильтры, шлюзы сеансового уровня, шлюзы прикладного уровня, межсетевые экраны экспертного уровня, персональные межсетевые экраны. Сетевой сканер XSpider. Система обнаружения вторжений Cisco IPS. | 4 |
| 7 | Системы анализа защищенности | Анализ угроз ИБ ресурсам интернета и причины их реализации Уязвимости операционных систем, серверов, рабочих станций, каналов связи. | 6 |
| 8 | Системы обнаружения и предотвращения вторжений | Сервисы безопасности: идентификация/аутентификация, разграничение доступа, протоколирование и аудит, экранирование, туннелированные, шифрование, контроль целостности, контроль защищенности, обнаружение отказов и оперативное восстановления, управление. | 6 |

5.2.3 Лабораторный практикум

| № п/п | Наименование раздела дисциплины | Тематика лабораторных работ | Трудоемкость, час |
|---|---|---|---|
| 1 | Уязвимость открытых систем на примере интернета | Работа со стандартными сетевыми утилитами. Работа с сетевым сканером и анализатором трафика. | 5 |
| 2 | Обеспечение информационной безопасности в открытых системах | Изучение и практическое применение шифрованной файловой системы LUKS и протокола удалённого управления ОС SSH. | 5 |
| 3 | Аутентификация субъектов и объектов взаимодействия в открытых системах | Работа с PAM, подключаемыми модулями аутентификации | 4 |
| 4 | Межсетевые экраны | Изучение и практическое применение межсетевого экрана ОС Linux Netfiler/iptables | 4 |

5.2.4 Самостоятельная работа обучающихся (СРО)

| № п/п | Наименование раздела дисциплины | Вид СРО | Трудоемкость, час |
|---|---|---|---|
| 1 | Стандартизация и модельное предоставление открытых информационных систем | Подготовка доклада с визуальным представлением (домашнее задание) | 8 |
| 2 | Уязвимость открытых систем на примере интернета | Подготовка к коллоквиуму (тестирование) | 4 |
| | | Подготовка отчетов по лабораторным и практическим работам | 6 |
| 3 | Атаки на открытые информационные системы | Подготовка к коллоквиуму (тестирование) | 4 |
| | | Подготовка отчетов по лабораторным и практическим работам | 6 |
| 4 | Обеспечение информационной безопасности в открытых системах | Подготовка к коллоквиуму (тестирование) | 4 |
| | | Подготовка отчетов по лабораторным работам | 5 |
| 5 | Аутентификация субъектов и объектов взаимодействия в открытых системах | Подготовка к коллоквиуму (тестирование) | 2 |
| | | Подготовка отчетов по лабораторным и практическим работам | 6 |
| 6 | Межсетевые экраны | Подготовка к коллоквиуму (тестирование) | 2 |
| | | Подготовка отчетов по лабораторным и практическим работам | 6 |
| 7 | Системы анализа защищенности | Расчетно-практическая работа | 8,1 |
| 8 | Системы обнаружения и предотвращения вторжений | | 10 |

## 6 Учебно-методическое и информационное обеспечение дисциплины

### 6.1 Основная литература

Мельников, Д.А. Информационная безопасность открытых систем [Электронный ресурс] : учебник. — Электрон. дан. — М. : ФЛИНТА, 2016. — 448 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=48368

Ковалев, Д.В. Информационная безопасность : учебное пособие / Д.В. Ковалев, Е.А. Богданова ; Министерство образования и науки РФ, Южный федеральный университет. – Ростов-на-Дону : Издательство Южного федерального университета, 2016. – 74 с. : схем., табл., ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=493175 (дата обращения: 30.01.2020). – Библиогр. в кн. – ISBN 978-5-9275-2364-1. – Текст : электронный.

**6.2 Дополнительная литература**

Инструменты безопасности с открытым исходным кодом. Хаулет Т. Национальный Открытый Университет «ИНТУИТ» 2016 г. – 566 с.

Безопасность информационных систем. Кияев В., Граничин О. Национальный Открытый Университет «ИНТУИТ» 2016. – 192 с.

Межсетевые экраны. Лапонина О.Р. Национальный Открытый Университет «ИНТУИТ» 2016. – 466 с.

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

Информационная безопасность открытых систем [Электронный ресурс]: методические указания для самостоятельной работы 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.vsuet.ru/ProtectedView/Book/ViewBook/1934.

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

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

**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. Данылив, Р. Н. Плотникова; ВГУИТ, Учебнометодическое управление. Воронеж : ВГУИТ, 2016. – Режим доступа : http://biblos.vsuet.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**

При изучении дисциплины используется программное обеспечение и информационные справочные системы: информационная среда для дистанционного обучения «Moodle», локальная сеть университета и глобальная сеть Internet, Libre Office 5.2 CodeBlocks; Oracle VM VirtualBox.

## 7 Материально-техническое обеспечение дисциплины

| | | |
|---|---|---|
| Аудитории для проведения занятий **лекционного** типа, лабораторных и практических занятий | Ауд. 420: Комплекты мебели для учебного процесса. ПЭВМ – 11 (компьютер Core i5-4460 – 10, Core i5-4570 – 1), рабочая станция РЕГАРД РДЦБ Core i5-8400 – 1 шт., 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-Р3.1»; 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; средство активной защиты информации изделие «Салют 2000С» с регулятором выходного уровня шума | Microsoft Windows 7 (академическая лицензия); Microsoft Office (standart) 2007; Microsoft Access 2007; Microsoft Project 2007; Microsoft Share Point 2007; Microsoft Visio 2007; Microsoft SQL server 2008; 7-Zip File Manager (архиватор); Adobe Acrobat Reader; Adobe Flash Player; FAR file manager; Google Chrome; Java TM 7 (64-bit); K-Lite Codec Pack; Mozilla Firefox; Oracle VM VirtualBox; Sublime Text; Symantec Endpoint Protection 12 (Заменен на AVP Kaspersky); VMWare Player; Антивирус “Зоркий глаз”; Lazarus; SmathStudio; NanoCAD; Gimp (графический редактор, аналог Photoshop); Avidemax (видео редактор); Virtual Dub (видео редактор); Free Pascal; Страж NT вер.4.0 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 |
| Аудитории для проведения занятий лекционного типа, **лабораторных и практических** занятий | Ауд. 332а: Комплекты мебели для учебного процесса. ПЭВМ – 12 (компьютер Core i5-4570), стенды – 5 шт.<br>Ауд. 424: Комплекты мебели для учебного процесса. ПЭВМ – 12: Моноблоки ГРАВИТОН М 40И Intel Pentium ® Gold G5420 CPU – 12 шт.; стенды – 3 шт.<br>Ауд. 420: Комплекты мебели для учебного процесса. ПЭВМ – 11 (компьютер Core i5-4460 – 10, Core i5-4570 – 1), рабочая станция РЕГАРД РДЦБ Core i5-8400 – 1 шт., 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-Р3.1»; система защиты речевой информации «Соната-АВ-4Б» (Центральный блок питания и управления + Размыкатели в составе СВАЗ Соната АВ); профессиональный обнаружитель скрытых видеокамер СОКОЛ-М (пере- | Ауд.332а:<br>ОС Alt Linux (Альт Образование 8.2)<br>Geany. Lazarus. Qt Creator. Quanta Plus. Веб-редактор 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.424:<br>ОС Alt Linux (Альт Образование 8.2)<br>Geany. Lazarus. Qt Creator. Quanta Plus. Веб-редактор 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 (академическая |

| | | |
|---|---|---|
| | носной); портативный обнаружитель закладок Protect1203 (переносной); устройство активной защиты информации «ВЕТО-М»; электронный замок Samsung SHS-2920 | лицензия), 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); K-Lite Codec Pack; Mozilla Firefox; Oracle VM VirtualBox; Sublime Text; Symantec Endpoint Protection 12 (Заменен на AVP Kaspersky); VMWare Player; Антивирус “Зоркий глаз”; Lazarus; SmathStudio; NanoCAD; Gimp (графический редактор, аналог Photoshop); Avidemax (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 С Сертификат ФСТЭК №2945 16.08.2013 |
| Аудитории для **самостоятельной** работы, курсового и дипломного проектирования | Читальные залы библиотеки: Компьютеры со свободным доступом в сеть Интернет и Электронными библиотечными и информационно справочными системами;<br>Ауд. 424: Комплекты мебели для учебного процесса. ПЭВМ – 1.; Моноблоки ГРАВИТОН М 40И Intel Prntium ® Gold G5420 CPU – 12 шт..; 3 стенда. | Microsoft Office Professional Plus 2010 Russian Academic OPEN 1 License No Level #61181017 от 20.11.2012 г. http://eopen.microsoft.com. Автоматизированная интегрированная библиотечная система «МегаПро», Номер лицензии: 104-2015, Дата: 28.04.2015. Договор №2140 от 08.04.2015 г. Уровень лицензии «Стандарт», ОС Alt Linux (Альт Образование 8.2)<br>Geany. Lazarus. Qt Creator. Quanta Plus. Веб-редактор 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. |
| Помещения для хранения и проф. обслуживания учебного оборудования | Ауд.423: ПЭВМ-3 (компьютер Core i5-4570 – 1 шт, компьютер Core i5-4460 – 1 шт., рабочая станция РЕГАРД РДЦБ Core i5-8400 – 1 шт , ноутбук 15,6HP, принтер Brother HL-2132, сетевой накопитель Dlink DNS-346 | Windows 7 (академическая лицензия) MS Office 2007 (open) |

## 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

по дисциплине

Информационная безопасность открытых 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 | ПК-3 | Способен проводить анализ защищенности автоматизированных систем | Основные методы и средства реализации удаленных сетевых атак на открытые информационные системы. Политики безопасности и меры защиты в открытых информационных системах | Работать с стандартными сетевыми утилитами. Работать с файловой системы LUKS и протокола удалённого управления ОС SSH. | Навыками анализа угроз и уязвимостей в открытых информационных системах. Навыками построения политик безопасности для открытых информационных систем |
| 2 | ОПК-4 | способностью понимать значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска информации в компьютерных системах, сетях, библиотечных фондах | Принципы работы сетевых протоколов и технологий передачи данных в открытых информационных системах. | Работать в UNIX-подобных системах | Терминологией и системным подходом построения защищенных открытых информационных систем. |

**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 | Стандартизация и модельное представление открытых информационных систем.<br>Уязвимость открытых систем на примере интранета.<br>Атаки на открытые информационные системы.<br>Обеспечение информационной безопасности в открытых системах | ПК-3 | Собеседование на экзамене | Проверка преподавателем |
| | | | Контрольные вопросы к текущим опросам на практических работах | Проверка преподавателем |
| | | | Темы докладов | Проверка преподавателем |
| 2 | Аутентификация субъектов и объектов взаимодействия в открытых системах.<br>Межсетевые экраны | ОПК-4 | Собеседование на экзамене | Проверка преподавателем |
| | | | Контрольные вопросы к текущим опросам на практических работах | Проверка преподавателем |
| | | | Вопросы к коллоквиуму | Проверка преподавателем |
| | | | Кейс-задания к лабораторным работам | Проверка преподавателем |

| | | | | |
|---|---|---|---|---|
| 3 | Системы анализа защищенности.<br>Системы обнаружения и предотвращения вторжений | ПК-3 | Собеседование на экзамене | Проверка преподавателем |
| | | | Контрольные вопросы к текущим опросам на практических работах | Проверка преподавателем |
| | | | Расчетно-практическая работа | Проверка преподавателем |

## 3 Оценочные средства для промежуточной аттестации

### 3.1 Вопросы к собеседованию на экзамене

ПК-3 – Способен проводить анализ защищенности автоматизированных систем

| № задания | Формулировка вопроса |
|---|---|
| 01 | Многофункциональные средства защиты открытых систем от сетевых атак |
| 02 | Основные элементы технологии открытых информационных систем |
| 03 | Совместимость открытых систем |
| 04 | Базовая модель информационной системы |
| 05 | Основные модели открытых систем |
| 06 | Понятие интранета. Структура интранета. Эталонная модель интранета. Этапы создания интранета. Виды интранета. Стандарты создания интранета |
| 07 | Интранет как часть среды открытых систем |
| 08 | Интранет и экстранет |
| 09 | Портал и интранет |
| 10 | Угрозы ресурсам интранета и причины их реализации |
| 11 | Уязвимость архитектуры клиент-сервер |
| 12 | Слабости системных утилит, команд и сетевых сервисов |
| 13 | Сетевые вирусы |
| 14 | Удаленные атаки на открытые системы |
| 15 | Типичные сценарии и уровни атак |

ОПК-4 - способностью понимать значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска информации в компьютерных системах, сетях, библиотечных фондах

| | |
|---|---|
| 16 | Классические и современные методы, используемые нападающими для проникновения в открытые системы |
| 17 | Четырехуровневая модель открытой системы |
| 18 | Специфика защиты ресурсов открытых систем на примере интранета |
| 19 | Системы анализа защищенности |
| 20 | Принципы создания защищенных средств связи объектов в открытых системах |
| 21 | Сервисы безопасности |
| 22 | Средства обеспечения информационной безопасности в открытых системах |
| 23 | Управление безопасностью открытых систем |
| 24 | Организационно-правовые методы защиты открытых систем |
| 25 | Аутентификация субъектов и объектов взаимодействия в открытых системах |
| 26 | Виртуальные вычислительные сети |
| 27 | Системы обнаружения и предотвращения вторжений |

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

ПК-3 – Способен проводить анализ защищенности автоматизированных систем

| № задания | Формулировка вопроса |
|---|---|
| 1. | Поведенческие системы обнаружения вторжений |
| 2. | Экранирование. Межсетевые экраны. Назначение и функции МЭ. |

| | |
|---|---|
| 3. | Основные компоненты МЭ. Принцип работы МЭ |
| 4. | Основные типы МЭ: пакетные фильтры, МЭ экспертного уровня. |
| 5. | Варианты размещения МЭ |
| 6. | Шлюзы сеансового уровня, шлюзы прикладного уровня |
| 7. | Руководящий документ Гостехкомиссии по МЭ. Требования к межсетевым экранам |
| 8. | Туннелирование |
| 9. | Базовая схема ВЧВС. Средства построения ВЧВС. |
| 10. | Механизм туннелирования как основа построения ВЧВС. |
| 11. | Общий поход к созданию туннелей, функции конкретных протоколов, участвующих в процессе туннелирования |
| 12. | ВЧВС на базе сетевой ОС, МЭ, маршрутизаторов, специализированного ПО, аппаратных средств – основные характеристики |
| 13. | Сравнительный анализ ВЧВС |
| 14. | Стандартные протоколы создания ВЧВС: канальный, сетевой, сеансовый уровни. |
| 15. | Политики безопасности для ВЧВС |
| 16. | Различные классификации ВСВЧ. Консорциум VPNC о VPN |
| 17. | Шифрование в интранете: аппаратное и программное; сетевые протоколы со встроенным шифрованием |
| 18. | Контроль целостности в интранете |
| 19. | Контроль защищенности интранета. Сетевые сканеры защищенности |
| 20. | Контроль защищенности интранета. Сканеры анализа защищенности: технологии сканирования, разновидности систем. Сканеры защищенности приложений |
| 21. | Обнаружение отказов и оперативное восстановление в интранете |
| 22. | Многофункциональные средства защиты открытых систем от сетевых атак |
| 23. | Системы обеспечения информационной безопасности на уровне организации |

ОПК-4 - способностью понимать значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска информации в компьютерных системах, сетях, библиотечных фондах

| | |
|---|---|
| 24. | Интеллектуальные системы обнаружения вторжений |
| 25. | Сетевые системы обнаружения вторжений |
| 26. | Хостовые системы обнаружения вторжений |
| 27. | Методы отражения вторжений. Системы обнаружения и предотвращения вторжений |
| 28. | Мониторинг и аудит ИБ в открытых системах |
| 29. | Средства идентификации/аутентификации в интранете |
| 30. | Комплексная эшелонированная защита интранета. |
| 31. | Средства обеспечения ИБ в сетях интранет |
| 32. | Топология сети: физическая изоляция; изоляция протокола; выделенные каналы. Сегментация сетей (демилитаризованная зона и "глубже"). |
| 33. | Реагирование на инциденты ИБ. |
| 34. | Нападения с использованием сетевых протоколов (spoofing, sniffing, flooding, hijacking, pharming…): предопределяющие уязвимости, признаки, защита |
| 35. | Перехват данных при их перемещении по каналам связи: средства, используемые уязвимости, защита. |
| 36. | Атака «Удаленный контроль над станцией в сети»: средства реализации, предопределяющие уязвимости, защита |
| 37. | Атаки «Отказ в обслуживании» и «Распределенный отказ в обслуживании» |
| 38. | Атака «Ложный объект распределенной вычислительной системы»: средства реализации, предопределяющие уязвимости, защита |
| 39. | Атака «Подмена доверенного объекта или субъекта распределенной вычислительной системы»: средства реализации, предопределяющие уязвимости, защита |
| 40. | Удаленные атаки на сети, их классификация. Типовые удаленные атаки. Атака «Анализ сетевого трафика»: средства реализации, предопределяющие уязвимости, защита |
| 41. | Электронная почта (серверы-клиенты-протоколы): уязвимости, угрозы ИБ, атаки, средства защиты |
| 42. | Угрозы ИБ, уязвимости и защита систем электронного документооборота |

| | |
|---|---|
| 43. | Угрозы ИБ, уязвимости и защита систем управления базами данных |

### 3.3. Расчетно-практическая работа

ПК-3 – Способен проводить анализ защищенности автоматизированных систем

| № задания | Формулировка задания |
|---|---|
| 1 | В работе следует разработать проект и построить модель защищенной корпоративной информационной системы, функционирующей на базе открытой информационной системы.<br>По итогам работы необходимо представить отчёт, включающий физическую и логическую топологию разработанной информационной системы, политику информационной безопасности, потенциальные уязвимости разработанной системы, обоснование выбора применяемых средств защиты (включая средства межсетевого экранирования, системы обнаружения атак, технологию построения виртуальной частной сети и др.), результаты моделирования.<br>Имитационное моделирование разработанной системы производится при помощи свободно распространяемых средств виртуализации |

### 3.4. Темы докладов

ПК-3 – Способен проводить анализ защищенности автоматизированных систем

| № задания | Формулировка задания |
|---|---|
| 1. | Политика использования ресурсов интранета |
| 2. | Политика в отношении паролей |
| 3. | Политика шифрования |
| 4. | Антивирусная политика |
| 5. | Политика оценки рисков |
| 6. | Политика аудита |
| 7. | Политика для пограничных маршрутизаторов |
| 8. | Политика удаленного доступа |
| 9. | Политика построения виртуальных частных сетей |
| 10. | Политика для экстранета |
| 11. | Политика для оборудования пограничной демилитаризованной зоны |
| 12. | Политика подключения подразделений к интранету |
| 13. | Политика подключения к интранету с применением модема |
| 14. | Политика для конфиденциальной информации |
| 15. | Политика для веб-сервера |
| 16. | Политика пересылки электронной почты |
| 17. | Политика хранения электронной почты |
| 18. | Политика для межсетевых экранов |
| 19. | Политика специального доступа |
| 20. | Политика подключения новых устройств в интранет |

### 3.5. Вопросы к коллоквиуму

ПК-3 – Способен проводить анализ защищенности автоматизированных систем

| № задания | Формулировка задания |
|---|---|
| 1. | Системы обеспечения информационной безопасности на уровне организации |
| 2. | Интеллектуальные системы обнаружения вторжений |
| 3. | Классификация и применение межсетевых экранов. |
| 4. | Межсетевой экран – пакетный фильтр. |
| 5. | Межсетевой экран – посредник прикладного уровня. |
| 6. | Назначение и возможности систем контроля содержания. |
| 7. | Обеспечение защиты информации средствами VPN. |
| 8. | Назначение и возможности систем анализа защищенности. |

| | |
|---|---|
| 9. | Назначение и возможности систем обнаружения совершенных атак. |
| 10. | Методы и средства контроля за действиями пользователей. |
| 11. | Методы защиты от несанкционированного изменения структур компьютерной системы. |

ОПК-4 - способностью понимать значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска информации в компьютерных системах, сетях, библиотечных фондах

| | |
|---|---|
| 12. | Защита от закладок при разработке программ. |
| 13. | Защита от несанкционированного изменения структур компьютерной системе в процессе эксплуатации. |
| 14. | Методы препятствующие использованию скопированной информации. |
| 15. | Защита программных средств от исследования. |
| 16. | Топология сети: физическая изоляция; изоляция протокола; выделенные каналы. Сегментация сетей (демилитаризованная зона и "глубже"). |
| 17. | Реагирование на инциденты ИБ. |

### 3.6. Кейс-задания на лабораторных работах

ПК-3 – Способен проводить анализ защищенности автоматизированных систем

| № задания | Формулировка задания |
|---|---|
| 1 | Изменение пароля пользователя не реже одного раза в 90 дней. |
| 2 | При смене пароля запрещается выбор в качестве нового какого-либо из последних четырех использовавшихся данным пользователем паролей. |
| 3 | Блокирование учетной записи после шести неудачных попыток ввода пароля. |
| 4 | Блокирование учетной записи пользователя не менее чем на 30 минут, либо пока администратор не снимет блокировку. |
| 5 | Использование в пароле не менее семи символов. |
| 6 | Использования в пароле как цифр, так и букв. |
| 7 | Настройте auditd для регистрации событий изменения системной даты и/или времени. Для этого вам потребуется отслеживать следующие системные вызовы: *adjtimex(), settimeofday(), stime(), clock_settime()*. Кроме того, необходимо отслеживать изменения файла */etc/localtime*. |
| 8 | Проверьте работоспособность правила при помощи команды date. |
| 9 | Настройте auditd для регистрации событий загрузки/выгрузки модулей ядра. Для этого вам потребуется отслеживать исполнение следующих файлов: */sbin/insmod*, */sbin/rmmod*, */sbin/modprobe*. Кроме того, необходимо отслеживать системные вызовы*init_module()* и *delete_module()*. |
| 10 | Получите отчёт auditd, демонстрирующий выполнение предыдущих заданий |
| 11 | Настройте OpenSSH для аутенфикации по открытому ключу. Для этого объединитесь в пары, сгенерируйте и обменяйтесь открытыми ключами при помощи команд, указанных выше. Проверьте работоспособность при помощи клиента ssh. Убедитесь в том, что трафик между компьютерами зашифрован при помощи tcpdump. |
| 12 | Передайте файл с одного компьютера на другой при помощи программы scp. С помощью снифера tcpdump убедитесь, что файл не передаётся по сети в открытом виде. |
| 13 | Передайте файл с одного компьютера на другой при помощи sftp |
| 14 | Настройте туннелирование трафика по протоколу SSH |
| 15 | Создайте шифрованную файловую систему в произвольном файле |
| 16 | Скопируйте в созданную ФС несколько текстовых файлов |
| 17 | Отключите шифрованную ФС. Просмотрите содержимое файла, содержащего шифрованную ФС и убедитесь, что данные не читаемы. |
| 18 | Подключите шифрованную ФС обратно |
| 19 | Фильтрация по критерию "источник":<br>iptables -I INPUT -s <IP-адрес или DNS-имя источника> -j {DROP/REJECT} [--reject-with reject_type]<br>Составьте правила для фильтрации входящего трафика с лабораторных машин с целями DROP и |

| | |
|---|---|
| | REJECT. При использовании цели REJECT проверьте влияние параметра *--reject-with*.<br>Убедитесь в работоспособности правил одним из доступных вам способов. |
| 20 | Фильтрация по критерию "протокол":<br>iptables -I INPUT -p {tcp/udp/icmp/all} -j {DROP/REJECT} [--reject-with reject_type]<br>Составьте правила для фильтрации входящего трафика с лабораторных машин с целями DROP и REJECT по протоколам tcp, udp и icmp. При использовании цели REJECT проверьте влияние параметра *--reject-with*.<br>Убедитесь в работоспособности правил одним из доступных вам способов. |
| 21 | Фильтрация по критерию "порт назначения":<br>iptables -I INPUT -p {tcp/udp} --dport <порт> -j {DROP/REJECT} [--reject-with reject_type]<br>Составьте правила для фильтрации входящего трафика с лабораторных машин с целями DROP и REJECT по протоколам tcp и udp с заданными портами. При использовании цели REJECT проверьте влияние параметра --reject-with.<br>Убедитесь в работоспособности правил одним из доступных вам способов |
| 22 | Фильтрация по критерию "входной интерфейс":<br>iptables -I INPUT -i <интерфейс> [-p <протокол>] -j {DROP/REJECT} [--reject-with reject_type]<br>Составьте правила для фильтрации входящего трафика на интерфейсе lo.<br>Убедитесь в работоспособности правил одним из доступных вам способов. |
| 23 | Маскировка машины путем блокирования ICMP-пакетов заданного типа:<br>iptables -I INPUT -p icmp --icmp-type <тип> -j DROP<br>Составьте правила для блокирования входящих ICMP-пакетов с типом Echo Request.<br>Убедитесь в работоспособности правил одним из доступных вам способов.<br>Примечание: список доступных типов ICMP можно посмотреть с помощью команды:<br>iptables -p icmp -h |
| 24 | Настройка простого межсетевого экрана с помощью iptables:<br>Составьте правила для следующей конфигурации межсетевого экрана:<br>Межсетевой экран должен блокировать все входящие соединения на внешний сетевой интерфейс (по любым протоколам), кроме входящих соединений на SSH-сервер (протокол TCP, порт 22)<br>Примечание: межсетевой экран не должен нарушать нормальную работу системы, все программы, требующие сетевого взаимодействия с удаленными хостами, должны работать (например, должны пинговаться удаленные хосты, работать веб-браузер, ftp-клиент и т.д.), т.е. "возвратные" пакеты в рамках установленных исходящих соединений не должны блокироваться.<br>Для проверки используйте утилиты ping и nmap.<br>TCP-сканирование nmap с другого компьютера должно определить один открытый порт (ssh) и все остальные фильтруемые.<br>TCP-сканирование nmap самого себя (localhost) не должно определять фильтруемых портов. |
| 25 | Настройте переадресацию пакетов с одного компьютера на другой. Для этого на компьютере, реализующем NAT, необходимо добавить соответствующее правило:<br>iptables -t nat -I PREROUTING -i <интерфейс> -s <входящий адрес> -j DNAT --to-destination <адрес переадресации><br>Проверьте работоспособность полученной системы. |
| 26 | Настройте SNAT |

## 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 |
| ПК-3 – Способен проводить анализ защищенности автоматизированных систем<br>ОПК-4 - способностью понимать значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска информации в компьютерных системах, сетях, библиотечных фондах | | | | | |
| ЗНАТЬ:<br>Основные методы и средства реализации удаленных сетевых атак на открытые информационные системы. Принципы работы сетевых протоколов и технологий передачи данных в открытых информационных системах. Политики безопасности и меры защиты в открытых информационных системах | 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) |
| | Коллоквиум | Уровень знаний | 85% и более правильных ответов | Отлично | Освоена (повышенный) |
| | | | 75-84% правильных ответов | Хорошо | Освоена (повышенный) |
| | | | 65-74% правильных ответов | Удовлетворительно | Освоена (базовый) |
| | | | Менее 64% правильных ответов | Не удовлетворительно | Не освоена (недостаточный) |
| УМЕТЬ:<br>Работать с стандартными сетевыми утилитами. Работать с файловой системы LUKS и протокола удалённого управления ОС SSH. Работать в UNIX-подобных системах | Контрольные вопросы к текущим опросам по 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) |
| | Кейс-задания на лабораторных | Уровень умения | студент выбрал верную методику решения задач, ответил на все вопросы, допустил не более 1 ошибки в ответе | Отлично | Освоена (повышенный) |

| | | | | | |
|---|---|---|---|---|---|
| | работ | | 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) |
| ВЛАДЕТЬ:<br>Навыками анализа угроз и уязвимостей в открытых информационных системах. Терминологией и системным подходом построения защищенных открытых информационных систем. Навыками построения политик безопасности для открытых информационных систем | 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) |
| | Расчетно-практическая работа | Уровень владения | 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) |