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

Система обнаружения компьютерных атак

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 задачи дисциплины «Система обнаружения компьютерных атак» в соответствии с видами профессиональной деятельности являются:

- эксплуатационную:

- реализация информационных технологий в сфере профессиональной деятельности с использованием защищенных автоматизированных систем;

- в соответствии со специализацией №4 «Безопасность открытых систем»:

- проектирование, эксплуатация и совершенствование системы управления информационной безопасностью открытой информационной системы.

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	Компетенция	Содержание компетенции (результат освоения)	В результате изучения учебной дисциплины обучающийся должен:		
			знать	уметь	владеть
1	ПК-3	способностью проводить анализ защищенности автоматизированных систем	основные задачи администрирования подсистемы ИБ объекта защита; инструменты администрирования;	проводить анализ угроз безопасности автоматизированных систем	моделями, методами и инструментами многослойной защиты информации
2	ПК-4	способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	Описание уязвимостей рассматриваемого объекта или ресурса.	использовать методы оценки уязвимости защищаемых персональных данных, построения модели угроз	методами построения модели угроз и нарушителей.
3	ПК-13	способностью участвовать в проектировании средств защиты информации автоматизированной системы	системы, комплексы и средства обеспечения информационной безопасности	проектировать комплексную систему защиты информации и информационных систем	методами и средствами проектирования систем обеспечения информационной безопасности и защиты информационных систем
4	ПК-14	способностью проводить контрольные провер-	основные программные, программно- аппарат-	организовывать и проводить контрольные проверки	методами и инструментами оценки эффективности

		ки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации	ные и технические средства защиты информации; основные метрологические показатели средств защиты информации	работоспособности средств защиты информации	
5	ПК-15	способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем	основные нормативные акты сертификации	находить и определять область применения различных категорий и видов стандартов, систем стандартов, классификаторов и указателей, документацией продукции, процессов, услуг и систем качества	навыками использования различных категорий и видов стандартов, систем стандартов, классификаторов и указателей, документацией продукции, процессов, услуг и систем качества
6	ПК-22	способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации	основные средства и способы обеспечения ИБ, принципы построения системы защиты ИБ	разрабатывать частные политики информационной безопасности информационных систем;	навыками разработки документирования, тестирования и отладки программного обеспечения по защите информации
7	ПК-23	способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа	применять методы и способы защиты информации в информационных системах персональных данных	определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности информационных систем, составлять аналитические обзоры по вопросам обеспечения информационной безопасности информационных систем;	навыками анализа информационной инфраструктуры информационной системы и ее безопасности
8	ПК-24	способностью обеспечить эффективное применение информационно- технологических ресурсов автоматизированной системы с учетом требований информационной безопасности	принципы организации информационны х систем в соответствии с требованиями по защите информации	разрабатывать частные политики информационной безопасности информационных (автоматизированных) систем	профессиональной терминологией в области информационной безопасности
9	ПК-25	способностью обеспечить эф-	принципы организации информа-	разрабатывать предложения по со-	навыками выбора и обоснования крите-

		фективное применение средств защиты информационно- технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных	ционных систем в соответствии с требованиями по защите информации	вершенствованию системы управления информационной безопасностью автоматизированных систем	риев эффективности функционирования защищенных информационных (автоматизированных) систем
10	ПК-27	способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы	подходы к формированию и реализации политики информационной безопасности автоматизированных систем	составлять политики информационной безопасности для автоматизированных систем и применять их на практике	навыками составления и использования политик информационной безопасности
11	ПК-28	способностью управлять информационной безопасностью автоматизированной системы	комплекс мероприятий по обеспечению информационной безопасности автоматизированных систем	определять перспективные направления и пути совершенствования автоматизированной системы	навыками участия в формировании, организации и поддержки комплекса мер по обеспечению информационной безопасности автоматизированной системы

3. Место дисциплины в структуре ОП ВО

Дисциплина «Система обнаружения компьютерных атак» относится к блоку 1 ОП и ее базовой части.

Изучение дисциплины основано на знаниях, умениях и навыках, полученных при изучении обучающимися базового школьного курса или освоении программы СПО.

Дисциплина является предшествующей для изучения дисциплин, прохождения практик:

- Безопасность сетей ЭВМ;
- Безопасность систем баз данных;
- Виртуальные частные сети;
- Защита web-сайтов;
- Защита конфиденциальной информации;
- Информационная безопасность открытых систем;
- Криптографические протоколы и стандарты;
- Криптографические методы защиты информации;
- Основы спектрального анализа;
- Программно-аппаратные средства обеспечения информационной безо-

пасности;

– Разработка и эксплуатация защищенных автоматизированных систем;

– Сети и системы передачи информации;

– Техническая защита информации;

– Элементы теории графов и сетей в математических пакетах;

– Учебная практика, практика по получению первичных профессиональных умений;

– Учебная практика, практика по получению первичных умений и навыков научно-исследовательской деятельности;

– Производственная практика, практика по получению профессиональных умений и опыта профессиональной деятельности;

– Производственная практика, преддипломная практика;

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

4. Объем дисциплины и виды учебных занятий

Общая трудоемкость дисциплины составляет 4 зачетные единицы.

Виды учебной работы	**Всего часов**	**Семестр**
		4
	акад. ч	акад. ч
Общая трудоемкость дисциплины	144	144
Контактная работа, в т.ч. аудиторные занятия	**55**	**55**
Лекции	18	18
в том числе в форме практической подготовки	–	–
Практические занятия (ПЗ)	36	36
в том числе в форме практической подготовки	36	36
Консультации текущие	0,9	0,9
Вид аттестации – зачет	0,1	0,1
Самостоятельная работа:	**89**	**89**
Проработка лекций, учебников (собеседование, коллоквиум)	40	40
Домашнее задание	49	49

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	Трудоемкость раздела, час
1	Теоретические основы	Модель OSI. Оборудование локальных сетей.	26
2	Классификация атак по уровням иерархической модели OSI	Атаки на физическом уровне. Атаки на канальном уровне; Атаки на сетевом уровне; Атаки на транспортном уровне; Безопасность прикладного уровня.	84
3	Уязвимости	Основные типы уязвимостей.	34

5.2 Разделы дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Лекции, час	ПЗ, час	СР, час
1	Теоретические основы	2	4	20
2	Классификация атак по уровням иерархической модели OSI	10	24	50
3	Уязвимости	6	8	20

5.2.1 Лекции

№ п/п	Наименование раздела дисциплины	Тематика лекционных занятий	Трудоемкость час
1	Теоретические основы	Модель OSI: Прикладной (7) уровень (Application Layer); представительский (6) уровень (Presentation Layer); Сеансовый (5) уровень (Session Layer); Транспортный (4) уровень (Transport Layer); Сетевой (3) уровень (Network Layer); Канальный (2) уровень (Data Link Layer); Физический (1) уровень (Physical Layer)	2
2	Классификация атак по уровням иерархической модели OSI	Атаки на физическом уровне. Концентраторы. Атаки на канальном уровне; Атаки на коммутаторы; Переполнение CAM-таблицы. VLAN Hoping Атака на STP; MAC Spoofing;Атака на PVLAN (Private VLAN) Атака на DHCP; ARP-spoofing; Атаки на сетевом уровне; Атаки на маршрутизаторы; Среды со статической маршрутизацией; Безопасность статической маршрутизации; Среды с динамической маршрутизацией; Scapy - универсальное средство дли реализации сетевых атак; Среды с протоколом RIP; Безопасность протокола RIP; Ложные маршруты RIP; Понижение версии протокола RIP; Взлом хэша MD5; Обеспечение безопасности протокола RIP; Среды с протоколом OSPF; Безопасность протокола OSPF; Среды с протоколом BGP; Атака BGP Router Masquerading; Атаки на MD5 для BGP; «Слепые» DoS-атаки на BGP- маршрутизаторы; Безопасность протокола BGP; Атаки на BGP; Атаки на транспортном уровне. Транспортный протокол TCP; Известные проблемы; Атаки на TCP; IP- spoofing; TCP hacking; Десинхронизация нулевыми данными; Сканирование сети; SYN-флуд; Атака Teardrop; Безопасность TCP; Атаки на уровне приложений. Безопасность прикладного уровня; Протокол SNMP; Протокол Syslog; Протокол DNS; Безопасность DNS; Веб- приложения; Атаки на веб через управление сессиями; Защита DNS; SQL-инъекции.	10
3	Уязвимости	Основные типы уязвимостей; Уязвимости проектирования; Уязвимости реализации; Уязвимости эксплуатации; Примеры уязвимостей; Права доступа к файлам; Оперативная память; Объявление памяти; Завершение нулевым байтом; Сегментация памяти программы; Переполнение буфера; Переполнения в стеке; Эксплоит без кода эксплоита; Переполнения в куче и bss; Перезапись указателей функций; Форматные строки; Сканирование приложений на наличие уязвимостей; Эксплуатация найденных уязвимостей; Защита от уязвимостей.	6

5.2.2 Практические занятия

№ п/п	Наименование раздела дисциплины	Тематика практических занятий	Трудоемкость, час
1	Теоретические основы	Работа с операционными системами Linux Server и Windows Server. Основные команды, приемы администрирования. Основы администрирования промышленных СУБД.	4
2	Классификация атак по уровням иерархической модели OSI	Работа с дистрибутивом диагностики и защиты сетей Kali Linux.	24
3	Уязвимости	Антивирусная диагностика и защита	8

5.2.3Лабораторный практикум Не предусмотрен

5.2.4 Самостоятельная работа обучающихся (СРО)

№ п/п	Наименование раздела дисциплины	Вид СРО	Трудоемкость, час
1	Теоретические основы	Проработка лекций, учебников (собеседование, коллоквиум)	10
		Подготовка отчетов по практической работе	10
2	Классификация атак по уровням иерархической модели OSI	Проработка лекций, учебников (собеседование, коллоквиум)	25
		Подготовка отчетов по практической работе	25
3	Уязвимости	Проработка лекций, учебников (собеседование)	10
		Подготовка отчетов по практической работе	10

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Основная литература

1. Бирюков, А.А. Информационная безопасность: защита и нападение / А.А. Бирюков. – 2-е изд., перераб. и доп. – Москва : ДМК Пресс, 2017. – 434 с. : ил., табл., схем. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=566834 (дата обращения: 16.02.2020). – ISBN 978-5-97060-435-9.

2. Артемов, А.В. Информационная безопасность : курс лекций / А.В. Артемов ; Межрегиональная Академия безопасности и выживания. – Орел : МАБИВ, 2014. – 257 с. : табл., схем. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=428605 (дата обращения: 16.02.2020). – Текст : электронный.

3. Прохорова, О.В. Информационная безопасность и защита информации : учебник / О.В. Прохорова ; Министерство образования и науки РФ, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Самарский государственный архитектурно-строительный университет». – Самара : Самарский государственный архитектурно- строительный университет, 2014. – 113 с. : табл., схем., ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=438331 (дата обращения: 16.02.2020). – Библиогр. в кн. – ISBN 978-5-9585-0603-3. – Текст : электронный.

4. Левкина, А.О. Компьютерные технологии в научно- исследовательской деятельности: учебное пособие для студентов и аспирантов социально- гуманитарного профиля / А.О. Левкина. – Москва ; Берлин : Директ-Медиа, 2018. – 119 с. : ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=496112 (дата обращения: 15.01.2020). – Библиогр. в кн. – ISBN 978-5-4475-2826-3. – DOI 10.23681/496112. – Текст : электронный.

6.2. Дополнительная литература

1. Скрипник, Д.А. Общие вопросы технической защиты информации / Д.А. Скрипник. – 2-е изд., испр. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 425 с. : ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=429070 (дата обращения: 16.02.2020). – Библиогр. в кн. – Текст : электронный.

2. Громов, Ю.Ю. Основы Web-инжиниринга: разработка клиентских приложений / Ю.Ю. Громов, О.Г. Иванова, С.В. Данилкин ; Министерство образования и науки Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Тамбовский государственный технический университет». – Тамбов : Издательство ФГБОУ ВПО

«ТГТУ», 2012. – 240 с. : ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=277648 (дата обращения: 15.01.2020). – Текст : электронный.

3. Голиков, А.М. Защита информации в инфокоммуникационных системах и сетях : учебное пособие / А.М. Голиков ; Министерство образования и науки Российской Федерации, Томский Государственный Университет Систем Управления и Радиоэлектроники (ТУСУР). – Томск : Томский государственный университет систем управления и радиоэлектроники, 2015. – 284 с. : схем., табл., ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=480637 (дата обращения: 16.02.2020). – Библиогр. в кн. – Текст : электронный.

6.3 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся

Защита web-сайтов [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.vsuet.ru/ProtectedView/Book/ViewBook/14820

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 высше- го образования / М. М. Данылив, Р. Н. Плотникова; ВГУИТ, Учебно-методическое управление. - Воронеж: ВГУИТ, 2016. – Режим доступа: http://biblos.vsuet.ru/MegaPro/Web/SearchResult/Marc Format/ 2488. - 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, Microsoft Office Professional Plus 2010 Microsoft Office Professional Plus 2007 Microsoft

Visual Studio; IIS 7+; .NET 4+

7 Материально-техническое обеспечение дисциплины (модуля)

Аудитории для проведения занятий лекционного типа, лабораторных и практических занятий	*Ауд. 420: Комплекты мебели для учебного процесса. ПЭВМ-12 (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 «НАВИГА-ТОР-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*	*Microsoft Windows 7 (64 разрядная) Профессиональная Лицензия (DreamSpark); Microsoft Office (standart) 2007 Профессиональная Лицензия (DreamSpark);Microsoft Access 2007 Профессиональная Лицензия (DreamSpark); Microsoft Project 2007 Профессиональная Лицензия (DreamSpark); Microsoft Share Point 2007 Профессиональная Лицензия (DreamSpark); Microsoft Visio 2007 Профессиональная Лицензия (DreamSpark) Microsoft SQL server 2008 Профессиональная Лицензия (DreamSpark); 1 С Предприятие Лицензия; 7-Zip File Manager (архиватор)Бесплатное ПО; Adobe Acrobat Reader (Бесплатное ПО); Adobe Flash Player (Бесплатное ПО); FAR file managerБесплатное ПО; Google ChromeБесплатное ПО; Java TM 7 (64-bit)Бесплатное ПО; K-Lite Codec PackБесплатное ПО; Mozilla FirefoxБесплатное ПО; Oracle VM VirtualBoxБесплатное ПО; Sublime TextБесплатное ПО; Symantec Endpoint Protection 12(Заменен на AVP Kaspersky)Бесплатное ПО; VMWare Player (Бесплатное ПО); Антивирус "Зоркий глаз" (Бесплатное ПО); Lazarus (аналог Delphi)Бесплатное ПО; SmathStudio (аналог Mathcad)Бесплатное ПО; NanoCAD (аналог Autocad)Бесплатное ПО; Gimp (графичский редактор аналог Photoshop) Бесплатное ПО; Avidemax (видео редактор)Бесплатное ПО; Virtual Dub (видео редактор)Бесплатное ПО; Free Pascal (Бесплатное ПО); Страж NT вер.3.0 Сертификат ФСТЭК No 2145 30.07.2013 г.; Ревизор 1XP Сертификат ФСТЭК No 989 08.02.2015 г.; Ревизор 2XP Сертификат ФСТЭК No 990 08.02.2015 г.; Фикс 2.0.2 Сертификат ФСТЭК No1548 15.01.2015 г.; Ревизор сети вер.3.0 Сертификат ФСТЭК No3413 02.06.2015 г.; СЗИ Панцирь К Сертификат ФСТЭК No1973 09.12.2015 г.; СЗИ Dallas Lock 8.0 К Сертификат ФСТЭК No2720 25.09.2015; СЗИ Dallas Lock 8.0 С Сертификат ФСТЭК No2945 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),средство активной защиты информации изделие «Салют 2000С» с регулятором выходного уровня шума, стенды – 5 шт. Ауд. 424: Комплекты мебели для учебного процесса. ПЭВМ – 12: рабочая станция CPU Core 2Duo E6300 – 1.86 – 10 шт, Celeron D2.8 – 2шт.; стенды – 3 Ауд. 420: Комплекты мебели для учебного процесса. ПЭВМ-12 (компьютер Core i5-4460), проектор Acer projector X1383WH, экран, стенды – 5 шт., блок управления комплекса радиоконтроля и поиска радиопередающих устройств «ОМЕГА» (перенос-*	*Microsoft Windows 7 (64 разрядная) Профессинальная Лицензия (DreamSpark); Microsoft Windows 2003 Профессиональная Лицензия (DreamSpark); Microsoft Office (standart) 2007 Профессиональная Лицензия (DreamSpark);Microsoft Access 2007 Профессиональная Лицензия (DreamSpark); Microsoft Project 2007 Профессиональная Лицензия (DreamSpark); Microsoft Share Point 2007 Профессиональная Лицензия (DreamSpark); Microsoft Visio 2007 Профессиональная Лицензия (DreamSpark) Microsoft SQL server 2008 Профессиональная Лицензия (DreamSpark); 1 С Предприятие Лицензия; 7-Zip File Manager (архиватор) Бесплатное ПО; Adobe Acrobat Reader Бесплатное ПО; Adobe Flash Player Бесплатное ПО; FAR file manager Бесплатное ПО;*

	ной), 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	*Google Chrome Бесплатное ПО; Java TM 7 (64-bit)Бесплатное ПО; K-Lite Codec Pack Бесплатное ПО; Mozilla Firefox Бесплатное ПО; Oracle VM VirtualBox Бесплатное ПО; Sublime Text Бесплатное ПО; Symantec Endpoint Protection 12 (Заменен на AVP Kaspersky) Бесплатное ПО; VMWare Player Бесплатное ПО; Антивирус "Зоркий глаз" Бесплатное ПО; Lazarus (аналог Delphi) Бесплатное ПО; Smath Studio (аналог Mathcad) Бесплатное ПО; NanoCAD (аналог Autocad) Бесплатное ПО; Gimp (графичский редактор аналог Photoshop) Бесплатное ПО; Avidemax (видео редактор) Бесплатное ПО; Virtual Dub (видео редактор) Бесплатное ПО; Free Pascal Бесплатное ПО (ауд.420) Страж NT вер.3.0 Сертификат ФСТЭК No 2145 30.07.2013 г.; Ревизор 1XP Сертификат ФСТЭК No 989 08.02.2015 г.; Ревизор 2XP Сертификат ФСТЭК No 990 08.02.2015 г.; Фикс 2.0.2 Сертификат ФСТЭК No1548 15.01.2015 г.; Ревизор сети вер.3.0 Сертификат ФСТЭК No3413 02.06.2015 г.; СЗИ Панцирь К Сертификат ФСТЭК No1973 09.12.2015 г.; СЗИ Dallas Lock 8.0 К Сертификат ФСТЭК No2720 25.09.2015; СЗИ Dallas Lock 8.0 С Сертификат ФСТЭК No2945 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; Ауд.424: Комплекты мебели для учебного процесса. Количество ПЭВМ – 12 (рабочая станция CPU Core 2Duo E6300 – 1.86 – 10 шт, Celeron D2.8 – 2 шт.), стенды – 3*	

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.

ОЦЕНОЧНЫЕМАТЕРИАЛЫ
ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

по дисциплине

Системы обнаружения компьютерных атак

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-4	способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	специфику возникновения угроз в открытых сетях; особенности защиты информации на узлах компьютерной сети, основные принципы построения систем обнаружения компьютерных атак	определять меры защиты информационных процессов в компьютерных системах; применять основные руководящие документы в области защиты информационных процессов в компьютерных системах	методикой выявления и анализа потенциально существующих угроз безопасности информации, составляющей государственную и другие виды тайны; способами настройки стандартных систем обнаружения компьютерных атак

2. Паспорт фонда оценочных средств по дисциплине

Контролируемые модули/разделы/темы дисциплины	Индекс контролируемой компетенции (или ее части)	Оценочные средства	Технология оценки (способ контроля)
Уязвимости традиционных средств защиты	ПК-4	Зачет	Зачтено-не зачтено
Этапы осуществления атаки		Контрольные вопросы к текущим опросам на практических работах	Уровневая шкала
Основные принципы обнаружения атак		Доклад	Уровневая шкала
Классификация систем обнаружения		Зачет	Зачтено-не зачтено
Обнаружение следов атак. Выбор системы обнаружения		Контрольные вопросы к текущим опросам на практических работах	Уровневая шкала
Размещение системы обнаружения атак		ДЗ № 1	Уровневая шкала
Аспекты создания системы обнаружения атак		Зачет	Зачтено-не зачтено
Реализация простейшей системы обнаружения атак		Контрольные вопросы к текущим опросам на практических работах	Уровневая шкала
		ДЗ № 2	Уровневая шкала

3. Оценочные средства для промежуточной аттестации

3.1 Вопросы к зачету

ПК-4 способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы

№ задания	Формулировка вопроса
1.	Основные угрозы информации в компьютерных системах.
2.	Особенности защиты информации на узлах компьютерной сети.
3.	Системы обнаружения атак. Назначение, основные виды, особенности использования.
4.	Уязвимости TCP/IP протокола.
5.	МЭ. Назначение, основные виды, особенности использования. Слабости МЭ, и способы его обхода
6.	Основные аспекты создания системы обнаружения атак.
7.	Сетевые сенсоры. Назначение, основные виды, особенности использования.
8.	Виртуальная частная сеть. Назначения, основные виды, особенности использования.
9.	Аутентификация и авторизация. Уязвимости аутентификации и авторизации.
10.	Классификация уязвимостей.
11.	Уязвимости платформы Windows.
12.	Классификация атак.
13.	Модель атаки. Этапы реализации атак.
14.	Что такое система обнаружения атак.
15.	Схема работы системы обнаружения.
16.	Признаки атак. Источники информации об атаках.
17.	Технологии и подходы к обнаружению атак.
18.	Анализ сетевого трафика.
19.	Анализ сервисов и портов.
20.	Системы анализа защищенности.
21.	Журнал регистрации. Назначение, особенности использования. Анализ журнала регистрации.
22.	Обманные системы. Назначение, особенности использования
23.	Системы контроля целостности.
24.	Предварительный анализ. Критерии оценки.
25.	Размещение системы обнаружения атак. Размещение сетевых сенсоров в коммутируемых сетях.

3.2 Контрольные вопросы к текущим опросам на практических работах

ПК-4 способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы

№ задания	Формулировка вопроса
1.	Перечислите основные угрозы информации в компьютерных системах.
2.	Перечислите особенности защиты информации на узлах компьютерной сети.
3.	Перечислите системы обнаружения атак.
4.	Уязвимости TCP/IP протокола?
5.	Что такое МЭ?
6.	Каковы основные аспекты создания системы обнаружения атак.
7.	Сетевые сенсоры.
8.	Виртуальная частная сеть.
9.	Аутентификация и авторизация. Уязвимости аутентификации и авторизации.
10.	Классификация уязвимостей.

11.	Уязвимости платформы Windows.
12.	Классификация атак.
13.	Модель атаки. Этапы реализации атак.
14.	Что такое система обнаружения атак.
15.	Схема работы системы обнаружения.
16.	Признаки атак. Источники информации об атаках.
17.	Технологии и подходы к обнаружению атак.
18.	Анализ сетевого трафика.
19.	Анализ сервисов и портов.
20.	Системы анализа защищенности.
21.	Журнал регистрации, его назначение
22.	Обманные системы.
23.	Системы контроля целостности.
24.	Предварительный анализ. Критерии оценки.
25.	Размещение системы обнаружения атак.
26.	Каково назначение систем обнаружения атак?
27.	Каковы основные виды систем обнаружения атак?
28.	Каковы особенности использования систем обнаружения компьютерных атак?
29.	Назначение, основные виды, особенности использования. Слабости МЭ, и способы его обхода
30.	Назначение сетевых сенсоров
31.	Основные виды сетевых сенсоров
32.	Особенности использования сетевых сенсоров
33.	Назначения виртуальных частных сетей
34.	Каковы основные виды виртуальных частных сетей?
35.	Каковы особенности использования виртуальных частных сетей?
36.	Размещение сетевых сенсоров в коммутируемых сетях.
37.	Анализ журнала регистрации.
38.	Назначение обманных систем
39.	Каковы особенности использования обманных систем
40.	Особенности использования журнала регистрации

3.3. Домашнее задание № 1

ПК-4 способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы

№ задания	Формулировка задания
1	1. Определить исходные данные (вид предприятия, краткое описание структуры предприятия, видов продукции и процессов, краткое описание инфраструктуры и ресурсов, описание информационной инфраструктуры предприятия). 2. Определить основные виды объектов защиты для данного предприятия. Для каждого вида объектов привести конкретные примеры. Объекты защиты выбирать в составе оборудования, инфраструктуры, персонала предприятия. 3. Определить основные виды угроз и способов их реализации для основных объектов защиты для заданного предприятия. 4. Для каждого вида угроз определить основные способы и средства предотвращения угроз. 5. Сформулировать основные элементы системы инженерно-технической защиты информации для заданного предприятия.

3.4. Темы докладов

ПК-4 способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы

№ задания	Формулировка задания
1.	Аппаратные средства обнаружения факта и места утечки конфиденциальной информации.
2.	Обзор межсетевые экраны.
3.	Виртуальные частные сети.
4.	Системы обнаружения атак.
5.	Особенности совместного использования процессами общих объектов в памяти.
6.	Использования шифрования для повышения защищённости компьютерных систем.
7.	Использование криптографического хеширования для контроля целостности программ и данных.
8.	Уязвимости различных платформ
9.	Обзор программных комплексов оценки рисков коммерческих информационных систем.
10.	Имитационная модель нарушителя информационной безопасности.
11.	Уязвимости платформы Windows
12.	Уязвимости платформы Linux

3.7. Домашнее задание № 2

ПК-4 способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы

№ задания	Формулировка задания
1	Встроенный межсетевой экран (firewall) Windows Server 2012. Персональный межсетевой экран появился в операционных системах семейства Windows, начиная с Windows XP / Windows Server 2003. В Windows Server 2012 возможности этого компонента существенно расширены, что позволяет более гибко производить настройки. Задание: 1. Откройте окно управления межсетевым экраном. Опишите действующие настройки. Создайте новое разрешающее правило. 2. Найдите правило, разрешающее отсылку ICMP-пакетов echo reguest. Проверьте его работу для какого-нибудь узла из локальной или внешней сети, используя его ip-адрес. Если ответ пришел, можно переходить ко второй части задания. Если ответа нет, попробуйте найти такой узел, который пришлет ответ. 3. Создайте правило, запрещающее отсылку icmp-пакетов на данный узел. Проверьте его работу. 4. Активируйте ведение журнала. Выполните команду ping для узла, для которого создавалось блокирующее правило. Проверьте содержимое файла журнала.

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-4 способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы					
ЗНАТЬ: специфику возникновения угроз в открытых сетях; особенности защиты информации на узлах компьютерной сети, основные принципы построения систем обнаружения компьютерных атак	Зачет	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)
	Доклад	Уровень знаний	выставляется студенту при наличии доклада, преобразовании информации в единую форму, презентации по выбранной теме, использованием не менее 10 источников, высоким уровнем владения представляемой информации	Отлично	Освоена (повышенный)
			выставляется студенту при наличии доклада, преобразовании информации в единую форму, презентации по выбранной теме, использованием менее 10 источников, низким уровнем владения представляемой информации	Хорошо	Освоена (повышенный)
			выставляется студенту при наличии доклада, презентации по выбранной теме, использованием менее 10 источников, не раскрытием поставленной задачи	Удовлетворительно	Освоена (базовый)
			выставляется студенту при наличии информации только из одного источника, и (или) отсутствии презентации по выбранной теме	Не удовлетворительно	Не освоена (недостаточный)
УМЕТЬ: определять меры защиты информационных процессов в компьютерных системах; при-	Контрольные вопросы к текущим	Уровень умения	студент выполнил задание и ответил на все вопросы и допустил не более 1 ошибки в ответе	Отлично	Освоена (повышенный)

менять основные руководящие документы в области защиты информационных процессов в компьютерных системах	опросам на практических работах		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: методикой выявления и анализа потенциально существующих угроз безопасности информации, составляющей государственную и другие виды тайны; способами настройки стандартных систем обнаружения компьютерных атак	Домашняя работа	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 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	Неудовлетворительно	Не освоена (недостаточный)