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

УТВЕРЖДАЮ
Проректор по учебной работе

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

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

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

«26» мая 2022

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Информационная безопасность открытых систем

Специальность

10.05.03 Информационная безопасность автоматизированных систем

Специализация

Безопасность открытых информационных систем

Квалификация (степень) выпускника

специалист по защите информации

Разработчик _____ _____ _____
(подпись) (дата) (Ф.И.О.)

СОГЛАСОВАНО:

Заведующий кафедрой информационной безопасности
(наименование кафедры, являющейся ответственной за данное направление подготовки, профиль)

_____ _____ Скрыпников А.В.
(подпись) (дата) (Ф.И.О.)

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 по-	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.	иска 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. Ауд. 424: Комплекты мебели для учебного процесса. ПЭВМ – 12: Моноблоки ГРАВИТОН М 40И Intel Pentium ® Gold G5420 CPU – 12 шт.; стенды – 3 шт. 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: 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, 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. Ауд.424: 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, 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. Ауд.420: 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; 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) 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.

АННОТАЦИЯ
К РАБОЧЕЙ ПРОГРАММЕ
ДИСЦИПЛИНЫ
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОТКРЫТЫХ СИСТЕМ
(наименование дисциплины)

Процесс изучения дисциплины направлен на формирование следующих компетенций:

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

– способен проводить анализ защищенности автоматизированных систем (ПК-3).

В результате освоения дисциплины студент должен:

Знать

– 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;

Уметь

– работать с стандартными сетевыми утилитами. Работать с файловой системы LUKS и протокола удалённого управления ОС SSH. Работать в UNIX-подобных системах;

Владеть

– 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.

Содержание разделов дисциплины. Основные элементы технологии открытых информационных систем. Совместимость открытых систем. Переносимость. Способность к взаимодействию. Основные модели открытых систем. Основные понятия. Угрозы ресурсам интранета 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. Удаленные атаки на открытые системы. Типичные сценарии и уровни атак. Специфика защиты ресурсов открытых систем на примере интранета. Выбор сетевой топологии интранета 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. Сетевая аутентификация «первый рубеж» защиты открытой системы. Подсистема аутентификации. Российский рынок средств аутентификации. 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. 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. Сетевое обнаружение вторжений. Поведенческое обнаружение вторжений. Интеллектуальное обнаружение вторжений. Комплексное обнаружение вторжений. Выбор системы обнаружения вторжений.