

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

УТВЕРЖДАЮ
Проректор по учебной работе

(подпись) Василенко В.Н.
(Ф.И.О.)

«26» мая 2022

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Программно-аппаратные средства обеспечения информационной безопасности

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 освоения дисциплины «Программно-аппаратные средства обеспечения информационной безопасности» являются:

эксплуатационная деятельность:

- реализация информационных технологий в сфере профессиональной деятельности с использованием защищенных автоматизированных систем;
- администрирование подсистем информационной безопасности автоматизированных систем.

контрольно-аналитическая:

- контроль работоспособности и эффективности применяемых средств защиты информации.

Объектами профессиональной деятельности являются:

- автоматизированные системы, функционирующие в условиях существования угроз в информационной сфере и обладающие информационно-технологическими ресурсами, подлежащими защите;
- информационные технологии, формирующие информационную инфраструктуру в условиях существования угроз в информационной сфере и задействующие информационно-технологические ресурсы, подлежащие защите;
- технологии обеспечения информационной безопасности автоматизированных систем;
- системы управления информационной безопасностью автоматизированных систем.

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

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

№п/п	Код компетенции	Содержание компетенции (результат освоения)	В результате изучения учебной дисциплины обучающийся должен:		
			знать	уметь	владеть
1	ОПК-8	способностью к освоению новых образцов программных, технических средств и информационных технологий	основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации	проектировать и администрировать компьютерные сети, реализовывать политику безопасности компьютерной сети	навыками использования программно-аппаратных средств обеспечения безопасности компьютерных сетей
2	ПК-25	способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций	основные протоколы компьютерных сетей	разрабатывать и администрировать базы данных и интерфейсы прикладных программ к базам данных	навыками анализа основных характеристик и возможностей телекоммуникационных систем по передаче информации

3. Место дисциплины в структуре ОП ВО

Дисциплина «Программно-аппаратные средства обеспечения информационной безопасности» относится к блоку 1 ОП ВО и ее базовой части.

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

- безопасность сетей ЭВМ;
- система обнаружения компьютерных атак;
- компьютерная и инженерная графика;
- мультимедиа технологии;
- Учебная практика, практика по получению первичных умений и навыков научно-исследовательской деятельности;
- Учебная практика, практика по получению первичных профессиональных умений.

Дисциплина является предшествующей для изучения дисциплин:

- техническая защита информации;
- виртуальные частные сети;
- производственная практика, преддипломная практика;
- защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты.

4. Объем дисциплины и виды учебных занятий

Общая трудоемкость дисциплины составляет 9 зачетных единиц.

Виды учебной работы	Всего часов	Семестр	
		7	8
	акад. ч	акад. ч	акад. ч
Общая трудоемкость дисциплины	324	144	180
Контактная работа , в т.ч. аудиторные занятия	148,7	91,6	57,1
Лекции	48	30	18
<i>в том числе в форме практической подготовки</i>	–	–	-
Лабораторные работы (ЛР)	30	30	-
<i>в том числе в форме практической подготовки</i>	30	30	-
Практические занятия (ПЗ)	66	30	36
<i>в том числе в форме практической подготовки</i>	66	30	36
Консультации текущие	4,6	1,5	0,9
Проведение консультаций перед экзаменом	2	–	2
Вид аттестации – зачет, экзамен	0,3	0,1	0,2
Самостоятельная работа	141,5	52,4	89,1
Подготовка доклада с презентацией	23	-	23
Домашнее задание № 1	25	25	-
Домашнее задание № 2	30	-	30
Домашнее задание № 3	36,1	-	36,1
Подготовка к коллоквиуму	27,5	27,5	-
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	Трудоемкость раздела, час
1	Общие сведения о программных и программно-аппаратных методах и средствах обеспечения информации	Цели и задачи курса. Содержание дисциплины. Рекомендуемая литература. Основные понятия и определения. Роль и место знаний по дисциплине «Программно-аппаратные средства обеспечения информационной безопасности» при освоении смежных дисциплин по выбранной специальности; в сфере профессиональной деятельности. Роль и место программно-аппаратных	8

	ционной безопасности	средств защиты информации в обеспечении информационной безопасности. Предмет и задачи программно-аппаратной защиты информации. Современный уровень и перспективы развития программно-аппаратных средств обеспечения информационной безопасности.	
2	Разграничение доступа	Избирательное разграничения доступа. Понятие матрицы доступа. Два подхода к кодированию матрицы доступа: векторы и списки. Изолированная программная среда. Полномочное разграничение доступа. Средства динамического изменения полномочий пользователя: необходимость, различные подходы к реализации.	22
3	Аутентификация	Правила безопасного хранения эталонной копии аутентификационной информации. Правила безопасной передачи по каналам связи аутентификационной информации. Понятие о специализированных сетевых протоколах безопасной аутентификации (Kerberos и т.п.). Проблемы парольной аутентификации. Методы подбора пароля. Средства защиты от подбора и компрометации паролей. Особенности аутентификации с использованием внешних носителей информации. Проблемы генерации и распределения ключей. Особенности биометрической аутентификации. Особенности аутентификации в системах управления базами данных. Реализация подсистем аутентификации в распространенных операционных системах.	20
4	Подсистема регистрации и учета	Необходимость регистрации и учета событий в защищенной автоматизированной системе. Основные требования к политике аудита. Требования к организации подсистемы аудита, к политике аудита. Настройка политики аудита в распространенных операционных системах.	32
5	Защита программ и данных от несанкционированного копирования	Задача защиты от несанкционированного копирования. Методы привязки к программно-аппаратной среде. Применение специальных аппаратных устройств (электронных ключей и т.п.) для защиты от несанкционированного копирования информации. Основные методы взлома систем защиты программ и данных от несанкционированного копирования: программная эмуляция эталонной программно-аппаратной среды, непосредственный взлом системы защиты («выкусывание» защитного кода).	32
6	Защита от вредоносных воздействий компьютерных вирусов и программных закладок	Основные типы компьютерных вирусов: файловые, сетевые, почтовые, макровирусы. Основные модели программных закладок: наблюдатель, перехват, искажение. Типичные признаки присутствия в системе компьютерных вирусов и программных закладок. Основные средства и методы противодействия компьютерным вирусам и программным закладкам: сигнатурное и эвристическое сканирование, контроль целостности, антивирусный мониторинг. Факторы, ограничивающие эффективность антивирусных средств.	30

5.2 Разделы дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Лекции, час	ЛР, час	ПЗ, час	СР, час
1	Общие сведения о программных и программно-аппаратных методах и средствах обеспечения информационной безопасности	2		6	
2	Разграничение доступа	10		12	
3	Аутентификация	8		12	

4	Подсистема регистрации и учета	10	10	12	
5	Защита программ и данных от несанкционированного копирования	10	10	12	
6	Защита от вредоносных воздействий компьютерных вирусов и программных закладок	8	10	12	

5.2.1 Лекции

№ п/п	Наименование раздела дисциплины	Тематика лекционных занятий	Трудоемкость, час
1	Общие сведения о программных и программно-аппаратных методах и средствах обеспечения информационной безопасности	Цели и задачи курса. Содержание дисциплины. Рекомендуемая литература. Основные понятия и определения. Роль и место знаний по дисциплине «Программно-аппаратные средства обеспечения информационной безопасности» при освоении смежных дисциплин по выбранной специальности; в сфере профессиональной деятельности. Роль и место программно-аппаратных средств защиты информации в обеспечении информационной безопасности. Предмет и задачи программноаппаратной защиты информации. Современный уровень и перспективы развития программноаппаратных средств обеспечения информационной безопасности.	2
2	Разграничение доступа	Избирательное разграничения доступа. Понятие матрицы доступа. Два подхода к кодированию матрицы доступа: векторы и списки. Изолированная программная среда. Полномочное разграничение доступа. Средства динамического изменения полномочий пользователя: необходимость, различные подходы к реализации.	10
3	Аутентификация	Правила безопасного хранения эталонной копии аутентификационной информации. Правила безопасной передачи по каналам связи аутентификационной информации. Понятие о специализированных сетевых протоколах безопасной аутентификации (Kerberos и т.п.). Проблемы парольной аутентификации. Методы подбора пароля. Средства защиты от подбора и компрометации паролей. Особенности аутентификации с использованием внешних носителей информации. Проблемы генерации и распределения ключей. Особенности биометрической аутентификации. Особенности аутентификации в системах управления базами данных. Реализация подсистем аутентификации в распространенных операционных системах.	8
4	Подсистема регистрации и учета	Необходимость регистрации и учета событий в защищенной автоматизированной системе. Основные требования к политике аудита. Требования к организации подсистемы аудита, к политике аудита. Настройка политики аудита в распространенных операционных системах.	10
5	Защита программ и данных от несанкционированного копирования	Задача защиты от несанкционированного копирования. Методы привязки к программно-аппаратной среде. Применение специальных аппаратных устройств (электронных ключей и т.п.) для защиты от несанкционированного копирования информации. Основные методы взлома систем защиты программ и данных от несанкционированного копирования: программная эмуляция эталонной программноаппаратной среды, непосредственный взлом системы	10

		защиты («выкусывание» защитного кода).	
6	Защита от вредоносных воздействий компьютерных вирусов и программных закладок	Основные типы компьютерных вирусов: файловые, сетевые, почтовые, макровирусы. Основные модели программных закладок: наблюдатель, перехват, искажение. Типичные признаки присутствия в системе компьютерных вирусов и программных закладок. Основные средства и методы противодействия компьютерным вирусам и программным закладкам: сигнатурное и эвристическое сканирование, контроль целостности, антивирусный мониторинг. Факторы, ограничивающие эффективность антивирусных средств.	8

5.2.2 Практические занятия

№	Наименование раздела дисциплины	Тематика практических занятий	Трудоемкость, час
1	Общие сведения о программных и программно-аппаратных методах и средствах обеспечения информационной безопасности	Администрирование, политики и компоненты системы безопасности в операционных системах семейства Windows.	6
2	Разграничение доступа	Разграничение доступа в операционных системах семейства Windows.	12
3	Аутентификация	Инструментальные средства настройки политики безопасности в ОС семейства Windows.	12
4	Подсистема регистрации и учета	Система защиты информации от несанкционированного доступа «Страж NT»	12
5	Защита программ и данных от несанкционированного копирования	Архитектура и функционирование шифрующей файловой системы EFS в ОС семейства Windows.	12
6	Защита от вредоносных воздействий компьютерных вирусов и программных закладок	Настройка системы аудита в ОС Windows.	12

5.2.3 Лабораторный практикум

№ п/п	Наименование раздела дисциплины	Тематика лабораторных занятий	Трудоемкость, час
1	Подсистема регистрации и учета	Контроль полномочий доступа к информационным ресурсам (Ревизор)	10
2	Защита программ и данных от несанкционированного копирования	Работа с программами защиты от несанкционированного копирования	10
3	Защита от вредоносных воздействий компьютерных вирусов и программных закладок	Работа с распространенными антивирусными средствами	10

5.2.4 Самостоятельная работа обучающихся (СРО)

№ п/п	Наименование раздела дисциплины	Вид СРО	Трудоемкость, час
1	Подсистема регистрации и учета Защита программ и данных от несанкционированного копирования	Домашнее задание № 1 «Разграничение доступа к информационным ресурсам»	25
		Подготовка к коллоквиуму	16
2	Защита от вредоносных воздействий компьютерных вирусов и программных закладок Аутентификация	Домашнее задание № 2	30
		Подготовка к коллоквиуму	11,5

3	Общие сведения о программных и программно-аппаратных методах и средствах обеспечения информационной безопасности Разграничение доступа	Домашнее задание № 3	36
		Подготовка доклада с визуальным представлением средствами PowerPoint	23

6 Учебно-методическое и информационное обеспечение дисциплины

6.1. Основная литература

1. Программно-аппаратные средства защиты информации : учебное пособие / Л. Х. Мифтахова, А. Р. Касимова, В. Н. Красильников [и др.]. – Санкт-Петербург : Интермедия, 2018. – 408 с. – ISBN 978-5-4383-0157-8. – Текст : электронный // Лань : электронно-библиотечная система. – URL: <https://e.lanbook.com/book/103200>

2. Маршаков, Д. В. Программно-аппаратные средства защиты информации : учебное пособие / Д. В. Маршаков, Д. В. Фатхи. – Ростов-на-Дону : Донской ГТУ, 2021. – 228 с. – ISBN 978-5-7890-1878-1. – Текст : электронный // Лань : электронно-библиотечная система. – URL: <https://e.lanbook.com/book/237770>

3. Фомин, Д. В. Информационная безопасность и защита информации: специализированные аттестованные программные и программно-аппаратные средства : методические указания / Д. В. Фомин. – Благовещенск : АмГУ, 2017. – 240 с. – Текст : электронный // Лань : электронно-библиотечная система. – URL: <https://e.lanbook.com/book/156494>

4. Костин, В. Н. Методы и средства защиты компьютерной информации: аппаратные и программные средства защиты информации : учебное пособие / В. Н. Костин. – Москва : МИСИС, 2018. – 21 с. – ISBN 978-5-906953-22-3. – Текст : электронный // Лань : электронно-библиотечная система. – URL: <https://e.lanbook.com/book/116744>

6.2. Дополнительная литература

1. Защита программ и данных : учебное пособие. – Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2020 – Часть 2 : Способы защиты анализа – 2020. – 52 с. – Текст : электронный // Лань : электронно-библиотечная система. – URL: <https://e.lanbook.com/book/180082>

2. Защита программ и данных : учебное пособие. – Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2020 – Часть 1 : Способы анализа – 2020. – 72 с. – Текст : электронный // Лань : электронно-библиотечная система. – URL: <https://e.lanbook.com/book/180081>

3. Программно-аппаратные средства защиты информации : учебно-методическое пособие / С. И. Штеренберг, А. М. Гельфанд, Д. В. Рыжаков, Р. А. Фатхутдинов. – Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2017. – 98 с. – Текст : электронный // Лань : электронно-библиотечная система. – URL: <https://e.lanbook.com/book/180093>

4. Воробьева, А. А. История развития программно-аппаратных средств защиты информации : учебное пособие / А. А. Воробьева, И. С. Пантюхин. – Санкт-Петербург : НИУ ИТМО, 2017. – 62 с. – Текст : электронный // Лань : электронно-библиотечная система. – URL: <https://e.lanbook.com/book/110499>

6.3 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся

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

2. Программно-аппаратные средства обеспечения информационной безопасности [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/1420>

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 «ВГУ-ИТ»	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. Данылиев, 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

Блок управления комплекса радиоконтроля и поиска радиопередающих устройств

«ОМЕГА» (переносной), МУ защиты ресурсов сети от внутренних и внешних атак CISCO ASA5505-KB, переносной комплекс для автоматизации измерений при проведении исследований и контроля технических средств ЭВТ «НАВИГАТОР-ПЗГ»; средство активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок

«СОНАТА-РЗ.1»; система защиты речевой информации «Соната-АВ-4Б» (Центральный блок питания и управления + Размыкатели в составе СВАЗ Соната АВ); профессиональный обнаружитель скрытых видеокамер СОКОЛ-М (переносной); портативный обнаружитель закладок Protect1203 (переносной); устройство активной защиты информации

«БЕТО-М»; электронный замок Samsung SHS-2920. Страж NT вер.3.0 Сер-

тификат ФСТЭК № 2145 30.07.2013 г.; Ревизор 1XP Сертификат ФСТЭК № 989 08.02.2015 г.; Ревизор 2XP Сертификат ФСТЭК № 990 08.02.2015 г.; Фикс 2.0.2 Сертификат ФСТЭК №1548 15.01.2015 г.; Ревизор сети вер.3.0 Сертификат ФСТЭК №3413 02.06.2015 г.; СЗИ Панцирь К Сертификат ФСТЭК №1973 09.12.2015 г.; СЗИ Dallas Lock 8.0 К Сертификат ФСТЭК №2720 25.09.2015; СЗИ Dallas Lock 8.0 С Сертификат ФСТЭК №2945 16.08.2013.

7. Материально-техническое обеспечение дисциплины

<p>Аудитории для проведения занятий лекционного типа, лабораторных и практических занятий</p>	<p>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-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; средство активной защиты информации изделие «Салют 2000С» с регулятором выходного уровня шума</p>	<p>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</p>
<p>Аудитории для проведения занятий лекционного типа, лабораторных и</p>	<p>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</p>	<p>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,</p>

<p>практических занятий</p>	<p>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-РЗ.1»; система защиты речевой информации «Соната-АВ-4Б» (Центральный блок питания и управления + Размыкатели в составе СВАЗ Соната АВ); профессиональный обнаружитель скрытых видеокамер СОКОЛ-М (переносной); портативный обнаружитель закладок Protect1203 (переносной); устройство активной защиты информации «ВЕТО-М»; электронный замок Samsung SHS-2920</p>	<p>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.</p> <p>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.</p> <p>Ауд.420: 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; 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); Avidemux (видео редактор); Virtual Dub (видео редактор); Free Pascal; Страж NT вер.3.0 Сертификат ФСТЭК № 2145 30.07.2013 г.; Ревизор 1XP Сертификат ФСТЭК № 989 08.02.2015 г.; Ревизор 2XP Сертификат ФСТЭК</p>
------------------------------------	---	--

		№ 990 08.02.2015 г.; Фикс 2.0.2 Сертификат ФСТЭК №1548 15.01.2015 г.; Ревизор сети ver.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
ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
(наименование дисциплины)**

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- способностью к освоению новых образцов программных, технических средств и информационных технологий (ОПК-8);
- способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций (ПК-25).

В результате освоения дисциплины студент должен:

Знать:

методы тестирования и отладки программного обеспечения, основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации, основные протоколы компьютерных сетей

Уметь:

проводить комплексное тестирование и отладку программных систем, проектировать и администрировать компьютерные сети, реализовывать политику безопасности компьютерной сети, разрабатывать и администрировать базы данных и интерфейсы прикладных программ к базам данных.

Владеть:

методиками оценки показателей качества и эффективности ЭВМ и вычислительных систем, навыками использования программно-аппаратных средств обеспечения безопасности компьютерных сетей, анализа основных характеристик и возможностей телекоммуникационных систем по передаче информации

Содержание разделов дисциплины.

Общие сведения о программных и программно-аппаратных методах и средствах обеспечения информационной безопасности. Разграничение доступа. Аутентификация

Подсистема регистрации и учета. Защита программ и данных от несанкционированного копирования. Защита от вредоносных воздействий компьютерных вирусов и программных закладок