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.)

«26» мая 2022

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Разработка и эксплуатация защищенных автоматизированных 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 (модуля)

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

контрольно-аналитическая:

контроль работоспособности и эффективности применяемых средств защиты информации;

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

проведение инструментального мониторинга защищенности автоматизированных систем и анализа его результатов.

Объектами профессиональной деятельности являются:

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

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

– технологии обеспечения информационной безопасности автоматизированных систем;

– системы управления информационной безопасностью автоматизированных систем.

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

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

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

3. Место дисциплины (модуля) в структуре ОП ВО

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

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

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

Дисциплина является предшествующей для изучения дисциплин:

- Аудит информационных технологий и систем обеспечения информационной безопасности;
- Безопасность облачных и распределенных вычислений;
- Гуманитарные аспекты информационной безопасности;
- Защита конфиденциальной информации;
- Производственная практика, преддипломная практика;

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

4. Объем дисциплины (модуля) и виды учебных занятий

Общая трудоемкость дисциплины составляет__4__ зачетных единицы.

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

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

5.1 Содержание разделов дисциплины

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

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

5.2 Разделы дисциплины и виды занятий

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

5.2.1 Лекции

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

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

5.2.2 Практические занятия

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

5.2.3 Лабораторный практикум

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

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

5.2.4 Самостоятельная работа обучающихся (СРО)

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

6 Учебно-методическое и информационное обеспечение дисциплины (модуля)

6.1. Основная литература

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

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

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

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

6.2. Дополнительная литература

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

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

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

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

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

6.3 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся

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

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

6.3 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся

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

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

Наименование ресурса сети «Интернет»	Электронный адрес ресурса
«Российское образование» федеральный портал	*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, Учебно-методическое 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

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

Блок управления комплекса радиоконтроля и поиска радиопередающих устройств «ОМЕГА» (переносной), МУ защиты ресурсов сети от внутренних и внешних атак CISCO ASA5505-KB, переносной комплекс для автоматизации измерений при проведении исследований и контроля технических средств ЭВТ «НАВИГАТОР-ПЗГ»; средство активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок «СОНАТА-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. Страж NT вер.3.0 Сертификат ФСТЭК № 2145 30.07.2013 г.; Ревизор 1XP Сертификат ФСТЭК № 989 08.02.2015 г.; Ревизор 2XP Сертификат ФСТЭК № 990 08.02.2015 г.; Фикс 2.0.2 Сертификат ФСТЭК №1548 15.01.2015 г.; Ревизор сети вер.3.0 Сертификат ФСТЭК №3413 02.06.2015 г.; СЗИ Панцирь К Сертификат ФСТЭК №1973 09.12.2015 г.; СЗИ Dallas Lock 8.0 К Сертификат ФСТЭК №2720 25.09.2015; СЗИ Dallas Lock 8.0 С Сертификат ФСТЭК №2945 16.08.2013.

7 Материально-техническое обеспечение дисциплины

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

	станция Регард РДЦБ.; стенды – 3 Ауд. 420: Комплекты мебели для учебного процесса. ПЭВМ-11 (компьютер Core i5-4460), проектор Acer projector X1383WH, экран, стенды – 5 шт., блок управления комплекса радиоконтроля и поиска радиопередающих устройств «ОМЕГА» (переносной), МУ защиты ресурсов сети от внутренних и внешних атак CISCO ASA5505-KB, переносной комплекс для автоматизации измерений при проведении исследований и контроля технических средств ЭВТ «НАВИГАТОР-ПЗГ»; средство активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок «СОНАТА-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	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. Вебредактор Bluefish. Среда разработки Code::Blocks. Офисный пакет Libre Office 5.4: Base, Calc, Draw, Impress, Math, Writer. Персональная бухгалтерия HomeBank. Словарь Star Dict. iTest. VM Maxima. Кумир. Avidemux. Audacios. Brasero. Cheese. SMPlayer. Медиаплеер Parole. Редактор тегов Easy TAG. Stath Studio. Pinta. Веб-браузер Mozilla Firefox. Графический редактор. FP – free Pascal. Ауд.420: Microsoft Windows 7 (64 разрядная) Microsoft Office (standart) 2007; Microsoft Access 2007; Microsoft Project 2007; Microsoft Share Point 2007; Microsoft Visio 2007; Microsoft SQL server 2008; 1 С Предприятие Лицензия; 7-Zip File Manager (архиватор); Adobe Acrobat Reader; Adobe Flash Player; FAR file manager; Google Chrome; Java TM 7 (64-bit); KLite Codec Pack; Mozilla Firefox; Oracle VM VirtualBox; Sublime Text; Symantec End-point Protection 12 (Заменен на AVP Kaspersky); VMWare Player; Антивирус “Зоркий глаз”; Lazarus; SmathStudio; NanoCAD; Gimp (графический редактор, аналог Photoshop); 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
Аудитория для самостоятельной работы студентов (Читальные залы библиотеки)	Компьютеры со свободным доступом в сеть Интернет и Электронным библиотечным и информационно-справочным системам	
Аудитория для групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации -	Комплекты мебели для учебного процесса – 30 шт., доска	
Аудитории для проведения занятий семинарского типа	Ауд. №332а: комп. класс каф. ИнфБ, количество ПЭВМ-12 (компьютер Cjrei5-4570, ауд.№ 420: комп.	ОС Alt Linux (Альт Образование 8.2) Geany. Lazarus. Qt Creator. Quanta Plus. Вебредактор Bluefish. Среда разработки Code::Blocks. Офисный пакет Libre Office 5.4: Base, Calc,

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

8 Оценочные материалы для промежуточной аттестации обучающихся по дисциплине

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

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

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

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

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

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

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

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

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

АННОТАЦИЯ
К РАБОЧЕЙ ПРОГРАММЕ
ДИСЦИПЛИНЫ
«РАЗРАБОТКА И ЭКСПЛУАТАЦИЯ ЗАЩИЩЕННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ»
(наименование дисциплины)

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- способностью применять нормативные правовые акты в профессиональной деятельности (ОПК-6);
- способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем (ПК- 15);
- способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности (ПК-20).

В результате освоения дисциплины обучающийся должен:

Знать

– методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем, функции операционных систем, основные концепции управления процессорами, памятью, вспомогательной памятью, устройствами, основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические), основы комплексного обеспечения информационной безопасности распределенных автоматизированных, информационно-управляющих систем;

Уметь

– администрировать подсистемы информационной безопасности автоматизированных систем, осуществлять сбор, обработку, анализ и систематизацию научно-технической информации в области ЭВМ и систем с применением современных информационных технологий, восстанавливать работоспособность подсистемы информационной безопасности автоматизированных систем в нештатных ситуациях; решать практические задачи информационной безопасности на основе инфраструктуры открытых ключей;

Владеть

– методами и технологиями проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных систем; навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем; навыками работы с современными инструментальными средствами для исследования программного обеспечения защищенных автоматизированных систем управления, развертывания и обеспечения работы программных комплексов, обеспечивающих работу с цифровыми сертификатами.

Содержание разделов дисциплины. Системный подход к построению защищенных автоматизированных систем. Понятие сложной системы. Управление и информация, самоорганизация. Основные принципы системного подхода при создании сложных систем; Понятие качества и эффективности. Методические вопросы оценки эффективности сложных систем. Функциональная и обеспечивающая часть сложной системы. Технология функционирования сложной системы. Угрозы безопасности локальных и распределённых автоматизированных систем. Проектирование автоматизированных систем. Цели и задачи проектирования. Структуризация предметной области. Классификация объектов проектирования. Жизненный цикл автоматизированной системы. Этапы проектирования системы. Организация работ, функции заказчиков и разработчиков. Проектирование и построение системы защиты автоматизированных систем. Практические методы реализации моделей безопасности. Ядра безопасности. Мониторинг взаимодействий в системе. Архитектура защищенных систем. Принципы построения защищенных информационных систем. Технологический цикл реализации защищенной системы обработки и хранения информации. Реализация систем контроля доступа; способы представления информации о правах доступа. Методология оценки защищенности изделий и продуктов информационных технологий. Критерии оценки безопасности информационных технологий. Контекст безопасности. Профиль защиты и задание по безопасности. Функциональные требования безопасности. Функциональные классы, семейства и компоненты безопасности. Требования доверия к безопасности. Классы, семейства и компоненты доверия. Оценочный уровень доверия. Критерии оценки профиля защиты и задания по безопасности.