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

Управление информационной безопасностью

Специальность

10.05.03 Информационная безопасность автоматизированных систем

Специализация

Безопасность открытых информационных систем

Квалификация выпускника

специалист по защите информации

1 Цели и задачи дисциплины

Целями и задачами освоения дисциплины «Управление информационной безопасностью» являются:

организационно-управленческая деятельность:

организация работы коллектива, принятие управленческих решений в условиях спектра мнений, определение порядка выполнения работ;

организационно-методическое обеспечение информационной безопасности автоматизированных систем;

организация работ по созданию, внедрению, эксплуатации и сопровождению защищенных 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	Код компетенции	Содержание компетенции (результат освоения)	В результате изучения учебной дисциплины обучающийся должен:		
			знать	уметь	владеть
1	ПК-12	способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы	методику управления инцидентами информационной безопасности; сущность аудита информационной безопасности	разрабатывать частные политики информационной безопасности	профессиональной терминологией в области информационной безопасности
2	ПК-28	способностью управлять информационной безопасностью автоматизированной системы	принципы управления логическим доступом к активам организации; принципы управления защищенной передачей данных; принципы управления безопасностью информационных систем	оценивать информационные риски	методами оценки информационных рисков

3 Место дисциплины в структуре ОП ВО

Дисциплина «Управление информационной безопасностью» относится к блоку 1 ОП и ее базовой части.

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

– Зарубежные стандарты по информационной безопасности;

– История криптографии;

– Учебная практика, практика по получению первичных профессиональ-

ных умений;

– Система обнаружения компьютерных атак.

Дисциплина является предшествующей для изучения дисциплин, прохождения практик:

– Основы управленческой 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 зачетных единиц.

Виды учебной работы	Всего часов	6 семестр
Общая трудоемкость дисциплины	**108**	**108**
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
Самостоятельная работа	**53**	**53**
Подготовка доклада с презентацией	23	23
Домашнее задание	20	20
Подготовка к коллоквиуму	10	10

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	Основы управления информационной безопасностью.	Основы построения систем обеспечения информационной безопасности на предприятии Деятельность по обеспечению информационной безопасности. Предметная направленность деятельности по обеспечению информационной безопасности. Цель деятельности по обеспечению информационной безопасности. Принципы и форма деятельности по обеспечению информационной безопасности. Методы деятельности по обеспечению информационной безопасности. Средства обеспечения информационной безопасности. Субъекты обеспечения информационной безопасности.	20
2	Управление рисками, инцидентами и аудит информаци-	Система управления информационной безопасностью бизнеса Модели непрерывного совершенствования и корпоративное управление. Модели непрерывного совершенствования и международные стандарты. Шаги реализации стандартной системы управления информационной безопасностью организации. Модели COSO, COBIT, ITIL. Контроль и аудит. Анализ и оценка управленческих и экономических показателей системы управления	31

	онной безопасности.	информационной безопасностью бизнеса Способы оценки информационной безопасности. Основные элементы процесса оценки информационной безопасности. Способы измерения атрибутов объекта оценки информационной безопасности. Применение типовых моделей оценки на основе оценки процессов и уровней зрелости процессов для оценки информационной безопасности. Модель оценки информационной безопасности на основе оценки процессов. Риск-ориентированная оценка информационной безопасности	
3	Рискология информационной безопасности	Цель процесса анализа рисков ИБ. Этапы и участники процесса анализа рисков ИБ. Разработка Методики анализа рисков ИБ. Инвентаризация активов. Понятие актива. Типы активов. Источники информации об активах организации. Выбор угроз ИБ и уязвимостей для выделенных на этапе инвентаризации активов. Оценка рисков ИБ. Планирование мер по обработке выявленных рисков ИБ. Утверждение результатов анализа рисков ИБ у высшего руководства. Использование результатов анализа рисков ИБ	34
4	Обеспечение соответствия требованиям законодательства РФ	Российское законодательство, затрагивающее аспекты и механизмы обеспечения безопасности в рамках СУИБ (авторское право, защита персональных данных и т.д.). Разработка процессов или дополнение существующих процессов управления ИБ с целью удовлетворения этим требованиям (необходимые документы, процессы, в которых данные требования могут быть выполнены)	22

5.2 Разделы дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Лекции, час	ПЗ, час	СР, час
1	Основы управления информационной безопасностью	4	8	8
2	Управление рисками, инцидентами и аудит информационной безопасности	4	12	15
3	Рискология информационной безопасности	6	8	20
4	Обеспечение соответствия требованиям законодательства РФ	4	8	10

5.2.1 Лекции

№ п/п	Наименование раздела дисциплины	Тематика лекционных занятий	Трудоемкость, час
1	Основы управления информационной безопасностью.	Основы построения систем обеспечения информационной безопасности на предприятии Деятельность по обеспечению информационной безопасности. Предметная направленность деятельности по обеспечению информационной безопасности. Цель деятельности по обеспечению информационной безопасности. Принципы и форма деятельности по обеспечению информационной безопасности. Методы деятельности по обеспечению информационной безопасности. Средства обеспечения информационной безопасности. Субъекты обеспечения информационной безопасности.	4
2	Управление рисками,	Система управления информационной безопасностью	4

	инцидентами и аудит информационной безопасности.	бизнеса Модели непрерывного совершенствования и корпоративное управление. Модели непрерывного совершенствования и международные стандарты. Шаги реализации стандартной системы управления информационной безопасностью организации. Модели COSO, COBIT, ITIL. Контроль и аудит. Анализ и оценка управленческих и экономических показателей системы управления информационной безопасностью бизнеса Способы оценки информационной безопасности. Основные элементы процесса оценки информационной безопасности. Способы измерения атрибутов объекта оценки информационной безопасности. Применение типовых моделей оценки на основе оценки процессов и уровней зрелости процессов для оценки информационной безопасности. Модель оценки информационной безопасности на основе оценки процессов. Риск-ориентированная оценка информационной безопасности	
3	Рискология информационной безопасности	Цель процесса анализа рисков ИБ. Этапы и участники процесса анализа рисков ИБ. Разработка Методики анализа рисков ИБ. Инвентаризация активов. Понятие актива. Типы активов. Источники информации об активах организации. Выбор угроз ИБ и уязвимостей для выделенных на этапе инвентаризации активов. Оценка рисков ИБ. Планирование мер по обработке выявленных рисков ИБ. Утверждение результатов анализа рисков ИБ у высшего руководства. Использование результатов анализа рисков ИБ	6
4	Обеспечение соответствия требованиям законодательства РФ	Российское законодательство, затрагивающее аспекты и механизмы обеспечения безопасности в рамках СУИБ (авторское право, защита персональных данных и т.д.). Разработка процессов или дополнение существующих процессов управления ИБ с целью удовлетворения этим требованиям (необходимые документы, процессы, в которых данные требования могут быть выполнены)	4

5.2.2 Практические занятия

№ п/п	Наименование раздела дисциплины	Тематика практических занятий	Трудоемкость, час
1	Основы управления информационной безопасностью.	Разработка и управление политикой ИБ информационной системы	8
2	Управление рисками, инцидентами и аудит информационной безопасности.	Анализ модели угроз ИБ и уязвимостей. Анализ модели информационных потоков	12
3	Рискология информационной безопасности	Обязательная документация системы управления информационной безопасностью (СУИБ). Процессы улучшения СУИБ («Внутренний аудит», «Корректирующие действия», «Предупреждающие действия»). Процесс «Мониторинг эффективности» (включая разработку метрик эффективности). Понятие «Зрелость процесса». Процесс «Анализ со стороны высшего руководства». Процесс «Обучение и обеспечение осведомленности»	8
4	Обеспечение соответствия требованиям законодательства РФ	Сертификация по ISO/IEC 27001 или ГОСТ Р ИСО/МЭК 27001. Период эксплуатации СУИБ перед сертификацией. Органы по сертификации, работающие в РФ (их	8

		различия и требования). Этапы сертификационного аудита. Решение о сертификации	

5.2.3 Лабораторный практикум
Не предусмотрен

5.2.4 Самостоятельная работа обучающихся (СРО)

№ п/п	Наименование раздела дисциплины	Вид СРО	Трудоемкость, час
1	Основы управления информационной безопасностью.	Подготовка к коллоквиуму	10
2	Обеспечение соответствия требованиям законодательства РФ		
3	Управление рисками, инцидентами и аудит информационной безопасности.	Подготовка доклада с визуальным представлением средствами PowerPoint	23
4	Рискология информационной безопасности	Домашнее задание	20

6 Учебно-методическое и информационное обеспечение дисциплины

6.1 Основная литература

1. Чекулаева, Е. Н. Управление информационной безопасностью : учебное пособие / Е. Н. Чекулаева, Е. С. Кубашева. — Йошкар-Ола : ПГТУ, 2020. — 154 с. — ISBN 978-5-8158-2165-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/157473

1. Крутиков, В.Н. Анализ данных : учебное пособие / В.Н. Крутиков, В.В. Мешечкин ; Министерство образования и науки Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Кемеровский государственный университет». - Кемерово : Кемеровский государственный университет, 2014. - 138 с. - URL: http://biblioclub.ru/index.php?page=book&id=278426

2. Жуковский, О.И. Информационные технологии и анализ данных : учебное пособие / О.И. Жуковский ; Министерство образования и науки Российской Федерации, Томский Государственный Университет Систем Управления и Радиоэлектроники (ТУСУР). - Томск : Эль Контент, 2014. - 130 с. http://biblioclub.ru/index.php?page=book&id=480500

3. Базы данных в высокопроизводительных информационных системах : учебное пособие / авт.- сост. Е.И. Николаев ; Министерство образования и науки РФ, Федеральное государственное автономное образовательное учреждение высшего образования «Северо-Кавказский федеральный университет». - Ставрополь : СКФУ, 2016. - 163 с. : - URL: http://biblioclub.ru/index.php?page=book&id=466799

6.2 Дополнительная литература

1. Поздняк, И. С. Управление информационной безопасностью : методические указания / И. С. Поздняк, И. С. Макаров. — Самара : ПГУТИ, 2019. — 43 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/223313

2. Туманов, В.Е. Проектирование хранилищ данных для систем бизнес-аналитики : учебное пособие / В.Е. Туманов. - Москва : Интернет-Университет Информационных Технологий, 2010. - 616 с. : ил., табл., схем. - (Основы информационных технологий). - URL: http://biblioclub.ru/index.php?page=book&id=233492

3. Добронец, Б.С. Численный вероятностный анализ неопределенных данных : монография / Б.С. Добронец, О.А. Попова ; Министерство образования и науки

Российской Федерации, Сибирский Федеральный университет. - Красноярск : Сибирский федеральный университет, 2014. - 168 с. URL: https://biblioclub.ru/index.php?page=book&id=435672

6.3 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся

1. Данылив, М. М. 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. – 32 с. Режим доступа в электронной среде: http://biblos.vsuet.ru/MegaPro/Web/SearchResult/MarcFormat/100813.

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 Project 2007, Microsoft Visio 2007, Microsoft Office (standart) 2007, 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»; СЗИ Dallas Lock 8.0 К; СЗИ Dallas Lock 8.0 С.

7 Материально-техническое обеспечение дисциплины

Аудитории для проведения занятий **лекционного** типа, лаборатор-	Ауд. 420: Комплекты мебели для учебного процесса. ПЭВМ-12 (компьютер Core i5-4460), проектор Acer projector	Microsoft Windows 7 (64 разрядная) Профессиональная Лицензия (DreamSpark); Microsoft Office (standart) 2007 Профессиональная Лицензия (DreamSpark);Microsoft Access 2007 Профессиональная Лицензия (DreamSpark); Microsoft Project

ных и практических занятий	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	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 ReaderБесплатное ПО; Adobe Flash Player Бесплатное ПО; FAR file managerБесплатное ПО; Google ChromeБесплатное ПО; Java TM 7 (64bit)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 PlayerБесплатное 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 PascalБесплатное ПО; 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 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	Microsoft Windows 7 (64 разрядная) Профессиональная 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 ReaderБесплатное ПО; Adobe Flash Player Бесплатное ПО; FAR file managerБесплатное ПО; Google ChromeБесплатное ПО; Java TM 7 (64bit)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 PlayerБесплатное ПО; Антивирус “Зоркий глаз”Бесплатное ПО; Lazarus (аналог Delphi)Бесплатное ПО; SmathStudio (аналог Mathcad)Бесплатное ПО; NanoCAD (аналог Autocad)Бесплатное ПО; Gimp (графичский редак-

	«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	тор аналог Photoshop)Бесплатное ПО; Avidemax (видео редактор)Бесплатное ПО; Virtual Dub (видео редактор)Бесплатное ПО; Free PascalБесплатное ПО (ауд.420) 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. Количество ПЭВМ – 12 (рабочая станция CPU Core 2Duo E6300 – 1.86 – 10 шт, Celeron D2.8 – 2 шт.), стенды – 3	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» 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 ReaderБесплатное ПО; Adobe Flash Player Бесплатное ПО; FAR file managerБесплатное ПО; Google ChromeБесплатное ПО; Java TM 7 (64bit)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 PlayerБесплатное 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

8 Оценочные материалы для промежуточной аттестации обучающихся по дисциплине

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

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

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

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

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

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

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

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

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

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

по дисциплине

Управление информационной безопасностью

(наименование дисциплины, практики в соответствии с учебным планом)

1 Перечень компетенций с указанием этапов их формирования

№п/п	Код компетенции	Содержание компетенции (результат освоения)	В результате изучения учебной дисциплины обучающийся должен:		
			знать	уметь	владеть
1	ПК-12	способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы	методику управления инцидентами информационной безопасности; сущность аудита информационной безопасности	разрабатывать частные политики информационной безопасности	профессиональной терминологией в области информационной безопасности
2	ПК-28	способностью управлять информационной безопасностью автоматизированной системы	принципы управления логическим доступом к активам организации; принципы управления защищенной передачей данных; принципы управления безопасностью информационных систем.	оценивать информационные риски	методами оценки информационных рисков

2 Паспорт фонда оценочных средств по дисциплине

№ п/п	Контролируемые модули/разделы/темы дисциплины	Индекс контролируемой компетенции (или ее части)	Оценочные средства	Технология оценки (способ контроля)
1	Основы управления информационной безопасностью	ПК-12	Зачет	Проверка преподавателем
			Контрольные вопросы к текущим опросам на практических работах	Проверка преподавателем
			Вопросы к коллоквиуму	Проверка преподавателем
2	Управление рисками, инцидентами и аудит информационной безопасности.	ПК-12	Зачет	Проверка преподавателем
			Контрольные вопросы к текущим опросам на практических работах	Проверка преподавателем
			Доклад	Проверка преподавателем
3	Рискология информационной безопасности	ПК-28	Зачет	Проверка преподавателем
			Контрольные вопросы к текущим опросам на практических работах	Проверка преподавателем
			ДЗ	Проверка преподавателем
4	Обеспечение соответствия требованиям законодательства РФ	ПК-12	Контрольные вопросы к текущим опросам на практических работах	Проверка преподавателем
			Вопросы к коллоквиуму	Проверка преподавателем

3. Оценочные средства для промежуточной аттестации

3.1 Вопросы к зачету

3.1.1. ПК-12 - способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы

№ задания	Формулировка вопроса
01	Процессный подход к построению СУИБ и циклическая модель PDCA.
02	Цели и задачи, решаемые СУИБ.
03	Стандартизация в области построения СУИБ: сходства и различия стандартов.
04	Стратегии выбора области деятельности СУИБ.
05	Стратегии построения СУИБ (построение системы в целом, построение отдельных процессов управления ИБ с последующим объединением в систему).
06	Основные этапы разработки СУИБ и роль руководства организации на каждом из этапов.
07	Политика ИБ и политика СУИБ: сходства и различия.
08	Распределение ролей и ответственности в рамках СУИБ: базовая ролевая структура, дополнительные роли в рамках процессов управления ИБ.
09	Анализ рисков ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
10	Анализ рисков ИБ: основные подходы, основные этапы процесса.
11	Управление инцидентами ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
12	Расследование инцидентов ИБ: виды расследования инцидентов, критерии выбора необходимого вида расследования, основные этапы расследования (для различных видов расследования).

3.1.2. ПК-28 - способностью управлять информационной безопасностью автоматизированной системы

13	Внутренние аудиты ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
14	Анализ со стороны руководства: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
15	Обучение и обеспечение осведомленности пользователей: цели и задачи процесса, роль процесса в рамках СУИБ.
16	Внедрение процессов управления ИБ: этапы и последовательность.
17	Ввод СУИБ в эксплуатацию: возможные проблемы и способы их решения

3.2 Контрольные вопросы к текущим опросам на практических работах

3.2.1. ПК-12 - способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы

№ задания	Формулировка вопроса
1.	Понятие СУИБ
2.	Объекты защиты информации.
3.	Основные задачи в рамках проблемы обеспечения безопасности информации, решаемые программно – аппаратными средствами защиты информации в ЭВМ.
4.	Угрозы информации в ЭВМ.
5.	Классификация угроз.
6.	Основные способы защиты информации в ЭВМ.
7.	Применение программно-аппаратных средств защиты информации от случайных угроз.
8.	Основные характеристики программно-аппаратных средств защиты информации.
9.	Классификация программно-аппаратных средств защиты информации.
10.	Компоненты компьютерной системы подверженные угрозам безопасности информации.
11.	Возможные угрозы доступа.
12.	Несанкционированный доступ к информации.
13.	Методы и средства ограничения доступа.

3.2.2. ПК-28 - способностью управлять информационной безопасностью автоматизированной системы

14.	Программно-аппаратные средства ограничения доступа.
15.	Привязка к аппаратным компонентам компьютерной системы.
16.	Привязка к логической организации данных в компьютерной системе.
17.	Методы и средства хранения ключевой информации (ключевые дискеты, электронные карточки и т.д.).
18.	Типовые решения в организации ключевых систем.
19.	Обоснование необходимости защиты программ от изучения.
20.	Способы анализа программ и методы противодействия изучению.
21.	Способы встраивания средств защиты в программное обеспечение.
22.	Понятие изолированной программной среды.
23.	Методы контроля целостности программ и данных.
24.	Защита информации от изменения.
25.	Программно-аппаратные средства обеспечения контроля целостности программ и данных.
26.	Основные виды компьютерных вирусов (классификация).
27.	Характеристика компьютерных вирусов.
28.	Способы обнаружения и защиты.
29.	Противодействие неизвестным компьютерным вирусам.
30.	Программные и аппаратные закладки.
31.	Противодействие внедрению закладок.
32.	Системные вопросы защиты программ и данных.
33.	Концепция защиты информации.
34.	Понятие комплексной защиты информации.
35.	Организационные вопросы обеспечения защиты информации.
36.	Основные критерии требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности.
37.	Современные требования руководящих документов в области защиты информации.
38.	Настроить параметры и провести поиск вирусов антивирусным средством NOD32.
39.	Настроить политику разграничения доступа в ОС Windows XP в соответствии с матрицей доступа.
40.	Зашифровать файлы с использованием файловой системы EFS.
41.	Настроить политику аутентификации пользователей в ОС Windows XP.
42.	Настроить подсистему регистрации и учета событий в ОС Windows XP.
43.	Настроить правила сетевой фильтрации в межсетевом экране Kerio WinRoute FireWall.
44.	Настроить параметры и провести поиск вирусов антивирусным средством NOD32.
45.	Настроить политику разграничения доступа в ОС Windows XP в соответствии с матрицей доступа.
46.	Зашифровать файлы с использованием файловой системы EFS.
47.	Настроить политику аутентификации пользователей в ОС Windows XP.
48.	Настроить подсистему регистрации и учета событий в ОС Windows XP.
49.	Настроить правила сетевой фильтрации в межсетевом экране Kerio WinRoute FireWall.

3.3. Домашнее задание

3.3.1. ПК-28 - способностью управлять информационной безопасностью автоматизированной системы

№ задания	Формулировка задания
1	Используя текст Конституции РФ, определите перечень прав и обязанностей граждан России в сфере информационной безопасности.
2	Охарактеризуйте сведения, составляющие государственную тайну, используя Закон РФ от 21 июля 1993 г. N 5485-I "О государственной тайне".
3	Приведите классификацию защищаемой информации на основании Федерального закона от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации".
4	Приведите систему законодательства об авторском праве и смежных правах.

5	Какую ответственность может понести нарушитель авторского права.
6	Приведите виды противоправных деяний в отношении компьютерной информации.
7	Используя Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ, назовите противоправные деяния в сфере защиты информации.
8	Используя Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 N 195-ФЗ определите виды нарушений правовых норм по защите информации.
9	Используя необходимые нормативные правовые документы приведите функции элементов организационной основы системы информационной безопасности РФ.
10	Создать контрольную точку для восстановления работоспособности компьютерной системы с операционной системой Windows.
11	Создать системный архив с помощью мастера архивации на персональном компьютере с операционной системой Windows.
12	Создать диск аварийного восстановления для персонального компьютера с операционной системой Windows.
13	Создать диск аварийного восстановления для персонального компьютера с операционной системой LINUX.
14	Создать образ системного диска персонального компьютера с использованием программы «Acronis».
15	Зарегистрировать нового пользователя и занести его в группу в операционной системе Windows.
16	Зарегистрировать нового пользователя и занести его в группу в операционной системе LINUX.
17	Разграничить доступ к файлу, директории и принтеру средствами операционной системы Windows.
18	Разграничить доступ к файлу, директории и принтеру средствами операционной системы LINUX.
19	Настроить аудит обращений к файлу от имени владельца средствами операционной системы Windows.
20	Настроить аудит обращений к файлу от имени владельца средствами операционной системы LINUX.
21	Настроить политику паролей средствами операционной системы Windows.
22	Настроить политику паролей средствами операционной системы LINUX.
23	Проверить компьютерную систему на наличие вредоносного программного обеспечения.

3.4. Темы докладов

3.4.1. ПК-12 - способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы

№ задания	Формулировка задания
1.	Управление непрерывностью деятельности: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
2.	Внутренние и внешние аудиты ИБ: цели и задачи процессов, сходства и различия.
3.	Российское законодательство, затрагивающее аспекты и механизмы обеспечения безопасности в рамках СУИБ, обеспечение соответствия требованиям законодательства.
4.	Документационное обеспечение СУИБ: понятия документа и записи, иерархия документов системы управления ИБ.
5.	Мониторинг эффективности мер по обеспечению ИБ и процессов управления ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
6.	Процессы улучшения системы управления ИБ: основные процессы, из взаимосвязь и роль в рамках СУИБ.
7.	Корректирующие/предупреждающие действия: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
8.	Классификация и структура нормативных правовых актов в сфере обеспечения информационной безопасности.
9.	Конституция и гражданский кодекс РФ о правах и обязанностях граждан России в сфере обес-

	печения информационной безопасности.
10.	Международное законодательство в области защиты информации.
11.	Международно-правовой опыт защиты информации.
12.	Информация и информационные системы – объекты правоотношений в сфере обеспечения информационной безопасности.
13.	Понятие и виды защищаемой информации.
14.	Правовая основа обеспечения защиты государственной тайны.
15.	Организация защиты государственной тайны.
16.	Защита интеллектуальной собственности в системе правового регулирования информационной безопасности.
17.	Основы авторского права.
18.	Основные положения патентного права.
19.	Организационно-правовая система обеспечения защиты объектов промышленной собственности на основе патентов.
20.	Основные положения Федерального закона РФ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите ин-формации».
21.	Основные положения Федерального закона РФ от 27.07.2006 № 152-ФЗ «О персональных данных».
22.	Правовая основа обеспечения защиты коммерческой тайны.
23.	Основные положения по защите коммерческой тайны.

3.5. Вопросы к коллоквиуму

3.5.1. ПК-12 - способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы

№ задания	Формулировка задания
1.	Задачи защиты информации в компьютерной системе от преднамеренных угроз.
2.	Задачи защиты информации в компьютерной системе от несанкционированного доступа.
3.	Способы и средства физической защиты ПЭВМ от несанкционированного доступа.
4.	Способы идентификации и аутентификации пользователей.
5.	Процедура контроля целостности аппаратной структуры компьютерной системы в процессе эксплуатации.
6.	Процедура контроля программной структуры компьютерной системы в процессе эксплуатации.
7.	Способы разграничения доступа к информации и компонентам ее обработки.
8.	Виды криптографического закрытия информации на запоминающих устройствах.
9.	Виды криптографического закрытия информации в процессе ее обработки (передачи).
10.	Методы и средства контроля за действиями пользователей.
11.	Методы защиты от несанкционированного изменения структур компьютерной системы.
12.	Защита от закладок при разработке программ.
13.	Защита от несанкционированного изменения структур компьютерной системе в процессе эксплуатации.
14.	Методы препятствующие использованию скопированной информации.
15.	Защита программных средств от исследования.
16.	Методы обнаружения известных и неизвестных вирусов.
17.	Методы удаления последствий заражения вирусами.
18.	Профилактика заражения вирусами компьютерной системы.
19.	Назначения и функции аппаратных модулей доверенной загрузки.
20.	Организационные меры защиты информации в компьютерной системе.
21.	Основы построения защищенных операционных систем.
22.	Угрозы безопасности операционной системы.
23.	Типичные атаки на операционную систему.
24.	Специфические угрозы безопасности информации в базах данных.
25.	Средства защиты баз данных.

26.	Разграничение доступа субъектов к объектам в операционной системе Windows.
27.	Атрибуты защиты объекта операционной системы Windows.
28.	Структура подсистемы аудита операционной системы Windows.
29.	Функции администратора по созданию и управлению учетными записями пользователей Windows.
30.	Политика и организация аудита ресурсов и событий системы защиты операционной системы Windows.
31.	Назначение и возможности настройки параметров безопасности защищенной операционной системы Windows.
32.	Разграничение доступа субъектов к объектам в операционной системе UNIX.
33.	Политика и организация аудита ресурсов и событий системы защиты операционной системы UNIX.
34.	Угрозы безопасности информации в сетях передачи данных. Прослушивание каналов связи.
35.	Угрозы безопасности информации в сетях передачи данных. Атака злоумышленник в середине.
36.	Угрозы безопасности информации в сетях передачи данных. Внедрение сетевых вирусов.
37.	Сетевые атаки на отказ в обслуживании.
38.	Основные механизмы защиты в сетях передачи данных.
39.	Назначение и способы сегментации локальных сетей.
40.	Классификация и применение межсетевых экранов.
41.	Межсетевой экран – пакетный фильтр.
42.	Межсетевой экран – посредник прикладного уровня.
43.	Назначение и возможности систем контроля содержания.
44.	Обеспечение защиты информации средствами VPN.
45.	Назначение и возможности систем анализа защищенности.
46.	Назначение и возможности систем обнаружения совершенных атак.
47.	Назначение и возможности систем обнаружения атак в процессе их реализации.

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-12 - способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы					
ЗНАТЬ: методику управления инцидентами информационной безопасности; сущность аудита информационной безопасности	Зачет	Уровень владения материалом	выставляется студенту при наличии доклада, преобразовании информации в единую форму, т.е. презентации по выбранной теме	Зачтено	Освоена (повышенный, базовый)
			выставляется студенту при наличии информации только из одного источника, и (или) отсутствии презентации по выбранной теме	Не зачтено	Освоена (недостаточный)
УМЕТЬ: разрабатывать частные политики информационной безопасности	Контрольные вопросы к текущим опросам по практическим работам	Уровень умения	студент выполнил задание и ответил на все вопросы и допустил не более 1 ошибки в ответе	Отлично	Освоена (повышенный)
			студент выполнил задание и ответил на все вопросы и допустил более 1 ошибки, но менее 3 ошибок	Хорошо	Освоена (повышенный)
			студент выполнил задание не полностью и ответил не на все вопросы, но в тех, на которые дал ответ не допустил ошибки	Удовлетворительно	Освоена (базовый)
			студент ответил не на все вопросы, допустил более 5 ошибок	Неудовлетворительно	Не освоена (недостаточный)
ВЛАДЕТЬ профессиональной терминологией в области информационной безопасности	Доклад	Уровень владения	выставляется студенту при наличии доклада, преобразовании информации в единую форму, т.е. презентации по выбранной теме	Зачтено	Освоена (повышенный, базовый)
			выставляется студенту при наличии информации только из одного источника, и (или) отсутствии презентации по выбранной теме	Не зачтено	Освоена (недостаточный)
	Коллоквиум	Владение терминологией в области информационной безопасности	студент выполнил задание и ответил на все вопросы и допустил не более 1 ошибки в ответе	Отлично	Освоена (повышенный)
			студент выполнил задание и ответил на все вопросы и допустил более 1 ошибки, но менее 3 ошибок	Хорошо	Освоена (повышенный)
			студент выполнил задание не полностью и ответил не на все вопросы, но в тех, на которые дал ответ не допустил ошибки	Удовлетворительно	Освоена (базовый)
			студент ответил не на все вопросы, допустил более 5 ошибок	Неудовлетворительно	Не освоена (недостаточный)
ПК-28 - способностью управлять информационной безопасностью автоматизированной системы					

ЗНАТЬ: принципы управления логическим доступом к активам организации; принципы управления защищенной передачей данных; принципы управления безопасностью информационных систем	Зачет	Уровень владения материалом	выставляется студенту при наличии доклада, преобразовании информации в единую форму, т.е. презентации по выбранной теме	Зачтено	Освоена (повышенный, базовый)
			выставляется студенту при наличии информации только из одного источника, и (или) отсутствии презентации по выбранной теме	Не зачтено	Освоена (недостаточный)
УМЕТЬ: оценивать информационные риски	Контрольные вопросы к текущим опросам по практическим работам	Уровень умения	студент выполнил задание и ответил на все вопросы и допустил не более 1 ошибки в ответе	Отлично	Освоена (повышенный)
			студент выполнил задание и ответил на все вопросы и допустил более 1 ошибки, но менее 3 ошибок	Хорошо	Освоена (повышенный)
			студент выполнил задание не полностью и ответил не на все вопросы, но в тех, на которые дал ответ не допустил ошибки	Удовлетворительно	Освоена (базовый)
			студент ответил не на все вопросы, допустил более 5 ошибок	Неудовлетворительно	Не освоена (недостаточный)
ВЛАДЕТЬ методами оценки информационных рисков	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	Не удовлетворительно	Не освоена (недостаточный)