МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ЛУГАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ ВЛАДИМИРА ДАЛЯ»

Институт управления и государственной службы
Кафедра производственного менеджмента

УТВЕРЖДАЮ:
Директор Института управления и
государственной службы
_____ Р.Г. Харьковский
(подпись)
«25» 04 2023 года

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

«Информационная безопасность предприятия и технологии защиты информации»

По направлению подготовки 38.04.02 Менеджмент

Магистерская программа «Управление организацией в цифровой экономике»

Луганск – 2023

Лист согласования РПУД

Рабочая программа учебной дисциплины «Информационная безопасность предприятия и технологии защиты информации» по направлению подготовки 38.04.02 Менеджмент, магистерская программа «Управление организацией в цифровой экономике» – 33 с.

Рабочая программа учебной дисциплины «Информационная безопасность предприятия и технологии защиты информации» разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки 38.04.02 «Менеджмент» (утвержден приказом Министерства образования и науки Российской Федерации от 12 августа 2020 г. № 952).

СОСТАВИТЕЛЬ:
канд. экон. наук, доцент, доцент кафедры
производственного менеджмента Щербакова Е.В.

Рабочая программа дисциплины утверждена на заседании кафедры производственного менеджмента «21» 03 2023 г., протокол № 11 .

Заведующий кафедрой
производственного менеджмента _____ Родионов А.В.

Переутверждена: «___»_____202__года, протокол № _____

Директор института
управления и государственной службы _____ Харьковский Р.Г.

Рекомендована на заседании учебно-методической комиссии института управления и государственной службы «12» 04 2023 г., протокол № 8 .

Председатель учебно-методической
комиссии института _____ Резник А.А.

Структура и содержание дисциплины

1. Цели и задачи дисциплины, ее место в учебном процессе

Целью изучения дисциплины «Информационная безопасность предприятия и технологии защиты информации» является углубленное изучение теоретических основ и методических аспектов в области информационной безопасности предприятия, изучение основных принципов, методов и средств защиты информации. При изучении практики внедрения информационной безопасности предприятия особое внимание уделяется углубленному изучению инструментов, методов и средств защиты информации.

Задачами изучения дисциплины «Информационная безопасность предприятий и технология защиты» являются: формирование у студентов базовой системы знаний в области информационной безопасности предприятия и инструментов, методов и средств защиты информации;

освоение основных понятий и терминологии информационной безопасности предприятия;

изучение нормативно-законодательной базы и стандартов информационной безопасности предприятия и технологии защиты информации;

изучение моделей информационной безопасности;

знакомство с угрозами, которым подвергается информация предприятия, а также классификацией этих угроз и их анализом;

изучение организационно-административных и технических методов и средств защиты информации;

изучение методов защиты информации;

обеспечение безопасности информационных систем;

обеспечение компьютерной и сетевой безопасности.

2. Место дисциплины в структуре ООП ВО

Дисциплина «Информационная безопасность предприятий и технология защиты информации» входит в часть, формируемую участниками образовательных отношений учебного плана. Необходимыми условиями для освоения дисциплины являются: знания принципов и закономерностей развития цифровой экономики; системное представление о современных концепциях управления организацией в цифровой среде; навыки реализации основных управленческих функций при помощи современных информационных и цифровых технологий.

Основывается на базе дисциплин: «Основы цифровой экономики», «Менеджмент в цифровой экономике», «Информационные технологии в управлении проектами».

Является основой для изучения следующих дисциплин: «Основы цифровой экономики», «Электронный документооборот», «Управление цифровыми рисками».

Дисциплина ориентирована на формирование знаний, умений и навыков, обеспечивающих построение в организации эффективной системы информационной безопасности предприятия и инструментов, методов и средств защиты информации на необходимом и достаточном уровне для достижения высокого уровня конкурентоспособности на рынке.

Курс «Информационная безопасность предприятия и технологии защиты информации» является необходимым для освоения общепрофессиональной и профессиональной компетенций по направлению подготовки 38.04.02 Менеджмент, а также, самостоятельного занятия научно-исследовательской работой студента и написания выпускной квалификационной работы – магистерской диссертации.

3. Требования к результатам освоения содержания дисциплины

Код и наименование компетенции	Индикаторы достижений компетенции (по реализуемой дисциплине)	Перечень планируемых результатов
ОПК-2. Способен применять современные техники и методики сбора данных, продвинутые методы их обработки и анализа, в том числе использовать интеллектуальные информационно - аналитические системы, при решении управленческих и исследовательских задач	**ОПК-2.1.** Знает современные технологии обработки информации. **ОПК-2.2.** Умеет решать управленческие и исследовательские задачи на основе информационной и библиографической культуры с применением информационно - коммуникационных технологий и с учетом основных требований информационной безопасности. **ОПК-2.3.** Владеет навыками количественного и качественного анализа информации при принятии управленческих решений.	**знать:** современные технологии обработки информации; принципы, методы и средства решения стандартных задач с учетом основных требований информационной безопасности; основные положения теории информационной безопасности на законодательном уровне; **уметь:** решать управленческие и исследовательские задачи на основе информационной и библиографической культуры с применением информационно - коммуникационных технологий и с учетом основных требований информационной безопасности; правильно выбирать и применять меры законодательного уровня для обеспечения информационной безопасности при решении стандартных задач профессиональной деятельности; **владеть:** навыками количественного и качественного анализа информации при принятии управленческих решений; навыками выбора и применения мер законодательного уровня информационной безопасности при решении стандартных задач профессиональной деятельности; навыками использования современных средств информационной безопасности при решении стандартных задач профессиональной деятельности

ПК-4. Способен выстраивать коммуникацию и кооперацию в цифровой среде на основе использования различных цифровых средств, позволяющих во взаимодействии с другими людьми достигать поставленных целей	**ПК-4.1.** Знает приемы коммуникации и кооперации в цифровой среде для постановки операционных целей и задач подразделениям организации. **ПК-4.2.** Умеет проводить оценку эффективности внедрения инновационных технологий в бизнес – процессы организации. **ПК-4.3.** Владеет способами формирования и построения структуры подразделений, методами осуществления изменений при построении структуры подразделений организации.	**знать:** приемы коммуникации и кооперации в цифровой среде для постановки операционных целей и задач подразделениям организации; виды и источники угроз безопасности информации при решении стандартных задач профессиональной деятельности; основные требования информационной безопасности при решении профессиональной деятельности; **уметь:** проводить оценку эффективности внедрения инновационных технологий в бизнес – процессы организации; определять актуальные источники угроз безопасности при решении стандартных задач профессиональной деятельности; **владеть:** способами формирования и построения структуры подразделений, методами осуществления изменений при построении структуры подразделений организации; навыками поиска необходимых нормативных и законодательных документов и навыками работы с ними при оформлении технической документации на различных стадиях жизненного цикла информационной системы

4. Структура и содержание дисциплины

4.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	**Объем часов (зач. ед.)**	
	Очная форма	**Заочная форма**
Общая учебная нагрузка (всего)	**144 (4 зач. ед)**	**144 (4 зач. ед)**
Обязательная аудиторная учебная нагрузка (всего) в том числе:	**36**	**14**
Лекции	12	6
Семинарские занятия	24	8
Практические занятия	-	-
Лабораторные работы	-	-
Курсовая работа (курсовой проект)	-	-
Другие формы и методы организации образовательного процесса (*расчетно-графические работы,* индивидуальные задания *и т.п.)*	-	-
Самостоятельная работа студента (всего)	**108**	**130**
Форма аттестации	**экзамен**	**экзамен**

4.2. Содержание разделов дисциплины

ТЕМА 1. ПОНЯТИЕ "ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ"

Проблема информационной безопасности общества. Определение понятия "информационная безопасность". Составляющие информационной безопасности

ТЕМА 2. СИСТЕМА ФОРМИРОВАНИЯ РЕЖИМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Задачи информационной безопасности общества. Уровни формирования режима информационной безопасности. Нормативно-правовые основы информационной безопасности в РФ

ТЕМА 3. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Классификация угроз "информационной безопасности". Вирусы как угроза информационной безопасности. Классификация компьютерных вирусов. Характеристика "вирусоподобных" программ. Антивирусные программы. Профилактика компьютерных вирусов. Обнаружение неизвестного вируса

ТЕМА 4. МЕХАНИЗМЫ ОБЕСПЕЧЕНИЯ "ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ"

Идентификация и аутентификация. Криптография и шифрование. Методы разграничение доступа. Регистрация и аудит. Межсетевое экранирование. Технология виртуальных частных сетей (VPN)

ТЕМА 5. МЕТОДЫ И ПРИЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

Современные угрозы информационной безопасности в России. Программные и технические средства защиты. Основные средства и методы защиты информации. Криптографические методы защиты информации. Сетевые методы защиты

ТЕМА 6. ЗАЩИТА ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Защита ПК от несанкционированного доступа. Опознавание (аутентификация) пользователей и используемых компонентов обработки информации. Цели защиты информации в сетях ЭВМ. Понятие сервисов безопасности. Понятие о служебной и государственной тайне. Симметрическое и ассиметричное шифрование

4.3. Лекции

№ п/п	Название темы	Объем часов	
		Очная форма	Заочная форма
1	Понятие "информационная безопасность"	2	1
2	Система формирования режима информационной безопасности	2	1
3	Угрозы информационной безопасности предприятия	2	1
4	Механизмы обеспечения "информационной безопасности"	2	1
5	Методы и приемы обеспечения информационной безопасности	2	1
6	Защита информации в информационных системах	2	1
Итого:		**12**	**6**

4.4. Практические (семинарские) занятия

№ п/п	Название темы	Объем часов	
		Очная форма	Заочная форма
1	Понятие "информационная безопасность"	4	1
2	Система формирования режима информационной безопасности	4	1
3	Угрозы информационной безопасности предприятия	4	1
4	Механизмы обеспечения "информационной безопасности"	4	2
5	Методы и приемы обеспечения информационной безопасности	4	2
6	Защита информации в информационных системах	4	1
Итого:		**24**	**8**

4.6. Самостоятельная работа студентов

№ п/п	Название темы	Вид СРС	Объем часов	
			Очная форма	Заочная форма
1	Понятие "информационная безопасность"	подготовка к текущей и промежуточной аттестации	18	22
2	Система формирования режима информационной безопасности	подготовка к текущей и промежуточной аттестации	18	22
3	Угрозы информационной безопасности предприятия	подготовка к текущей и промежуточной аттестации	18	22
4	Механизмы обеспечения "информационной безопасности"	подготовка к текущей и промежуточной аттестации	18	22
5	Методы и приемы обеспечения информационной безопасности	подготовка к текущей и промежуточной аттестации	18	22
6	Защита информации в информационных системах	подготовка к текущей и промежуточной аттестации	18	20
Итого:			**108**	

4.7. Курсовые работы/проекты по дисциплине «Цифровой маркетинг» не предполагаются учебным планом.

5. Образовательные технологии

Преподавание дисциплины ведется с применением следующих видов образовательных технологий:

традиционные объяснительно-иллюстративные технологии, которые обеспечивают доступность учебного материала для большинства студентов, системность, отработанность организационных форм и привычных методов, относительно малые затраты времени;

технологии проблемного обучения, направленные на развитие познавательной активности, творческой самостоятельности студентов и предполагающие последовательное и целенаправленное выдвижение перед студентом познавательных задач, разрешение которых позволяет студентам активно усваивать знания (используются поисковые методы; постановка познавательных задач);

технологии развивающего обучения, позволяющие ориентировать учебный процесс на потенциальные возможности студентов, их реализацию и развитие;

технологии концентрированного обучения, суть которых состоит в создании максимально близкой к естественным психологическим особенностям человеческого восприятия структуры учебного процесса и которые дают возможность глубокого и системного изучения содержания учебных дисциплин за счет объединения занятий в тематические блоки;

технологии модульного обучения, дающие возможность обеспечения гибкости процесса обучения, адаптации его к индивидуальным потребностям и особенностям обучающихся (применяются, как правило, при самостоятельном обучении студентов по индивидуальному учебному плану);

технологии дифференцированного обучения, обеспечивающие возможность создания оптимальных условий для развития интересов и способностей студентов, в том числе и студентов с особыми образовательными потребностями, что позволяет реализовать в культурно-образовательном пространстве университета идею создания равных возможностей для получения образования

технологии активного (контекстного) обучения, с помощью которых осуществляется моделирование предметного, проблемного и социального содержания будущей профессиональной деятельности студентов (используются активные и интерактивные методы обучения) и т.д.

Максимальная эффективность педагогического процесса достигается путем конструирования оптимального комплекса педагогических технологий и (или) их элементов на личностно-ориентированной, деятельностной, диалогической основе и использования необходимых современных средств обучения.

7. Учебно-методическое и информационное обеспечение дисциплины:

а) основная литература:

1. Ковалев, Д. В. Информационная безопасность: Учебное пособие / Ковалев Д.В., Богданова Е.А. - Ростов-на-Дону:Южный федеральный университет, 2016. - 74 с.: ISBN 978-5-9275-2364-1. - Текст : электронный. - URL: https://znanium.com/catalog/product/997105 (дата обращения: 23.08.2023). – Режим доступа: по подписке.

2. Баранова, Е. К. Информационная безопасность. История специальных методов криптографической деятельности : учебное пособие / Е.К. Баранова, А.В. Бабаш, Д.А. Ларин. — Москва : РИОР : ИНФРА-М, 2024. — 236 с. - ISBN 978-5-369-01788-3. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2140687 (дата обращения: 26.08.2023). – Режим доступа: по подписке.

3. Информационная безопасность: вчера, сегодня, завтра : материалы V Международной научно-практической конференции (Москва, 14 апреля 2022 г.) / под ред. В. В. Арутюнова. - Москва : РГГУ, 2022. - 191 с. - ISBN 978-5-7281-3105-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/1991966 (дата обращения: 21.08.2023).

4. Котенко, В. В. Теория информации и защита телекоммуникаций:: монография / Котенко В.В., Румянцев К.Е. - Ростов-на-Дону:Издательство ЮФУ, 2009. - 369 с. ISBN 978-5-9275-0670-5. - Текст : электронный. - URL: https://znanium.com/catalog/product/556817 (дата обращения: 21.08.2023). – Режим доступа: по подписке.

5. Клименко, И. С. Информационная безопасность и защита информации: модели и методы управления : монография / И.С. Клименко. — Москва : ИНФРА-М, 2024. — 180 с. — (Научная мысль). — DOI 10.12737/monography_5d412ff13c0b88.75804464. - ISBN 978-5-16-015149-6. -

Текст : электронный. - URL: https://znanium.com/catalog/product/2052391 (дата обращения: 19.08.2023). – Режим доступа: по подписке.

б) дополнительная литература:

1. Информационная безопасность : лабораторный практикум / составители Т. Н. Катанова, Л. С. Галкина, Р. А. Жданов. — Пермь : Пермский государственный гуманитарно- педагогический университет, 2018. — 86 с. — ISBN 978-5-85219-007-9. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/86357.html

2. Комплексное обеспечение информационной безопасности автоматизированных систем: лабораторный практикум / М. А. Лапина, Д. М. Марков, Т. А. Гиш [и др.]. — Ставрополь: Северо-Кавказский федеральный университет, 2016. — 242 с. — ISBN 2227- 8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/62945.html

3. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов: учеб. пособие / Ю.Н. Сычев. — М. : ИНФРА-М, 2019. — 223 с. — (Высшее образование: Бакалавриат). — www.dx.doi.org/10.12737/textbook_5cc15bb22f5345.11209330. - Режим доступа: http://znanium.com/catalog/product/979415

4. Фаронов, А. Е. Основы информационной безопасности при работе на компьютере / А. Е. Фаронов. — М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 154 с. — ISBN 2227-8397. — Текст : электронный // Электронно- библиотечная система IPR BOOKS : [сайт]. — Режим доступа: http://www.iprbookshop.ru/52160.html.

5. Фомин, Д. В. Информационная безопасность: учебно-методическое пособие для студентов-бакалавров укрупненной группы направлений подготовки 38.00.00 «Экономика и управление» / Д. В. Фомин. — Саратов: Вузовское образование, 2018. — 82 с. — ISBN 978-5-4487-0300-3. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — Режим доступа: http://www.iprbookshop.ru/77319.html.

6. Авдошин, С. М. Технологии и продукты Microsoft в обеспечении информационной безопасности / С. М. Авдошин, А. А. Савельева, В. А. Сердюк. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017. — 412 с. — ISBN 978-5-4487-0147-4. — Текст : электронный // Электронно- библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/72341.html

7. Информационная безопасность. История специальных методов криптографической деятельности: Учебное пособие / Баранова Е.К., Бабаш А.В., Ларин Д.А. - М.:ИЦ РИОР, НИЦ ИНФРА-М, 2019. - 236 с.: - Режим доступа: http://znanium.com/catalog/product/987215

8. Суворова, Г. М. Информационная безопасность : учебное пособие / Г. М. Суворова. — Саратов : Вузовское образование, 2019. — 214 с. — ISBN 978-5-4487-0585-4. — Текст : электронный // Электронно-библиотечная система IPR

BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/86938.html. — Режим доступа: для авторизир. пользователей

9. Фомин, Д. В. Методические указания и индивидуальные задания для самостоятельной работы по дисциплине Комплексное обеспечение информационной безопасности инфокоммуникационных сетей и систем / составители И. Л. Боброва, К. А. Севрук. — М. : Московский технический университет связи и информатики, 2015. — 35 с. — ISBN 2227- 8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — Режим доступа: http://www.iprbookshop.ru/61737.html.

в) Интернет-ресурсы:

Министерство образования и науки Российской Федерации – http://минобрнауки.рф/

Федеральная служба по надзору в сфере образования и науки – http://obrnadzor.gov.ru/

Министерство образования и науки Луганской Народной Республики – https://minobr.su

Информационно-аналитическая система – http://www.spark-interfax.ru

Информационная система «Единое окно доступа к образовательным ресурсам» – http://window.edu.ru/

Народный совет Луганской Народной Республики – https://nslnr.su

Портал Федеральных государственных образовательных стандартов высшего образования – http://fgosvo.ru

Федеральный портал «Российское образование» – http://www.edu.ru/

Федеральный центр информационно-образовательных ресурсов – http://fcior.edu.ru/

Электронно-библиотечная система «Консультант-студента» – http://www.studentlibrary.ru/cgi-bin/mb4x

Электронно-библиотечная система «StudMed.ru» –https://www.studmed.ru

Информационный ресурс библиотеки образовательной организации

Научная библиотека имени А. Н. Коняева – http://biblio.dahluniver.ru/

8. Материально-техническое и программное обеспечение дисциплины

Освоение дисциплины «Информационная безопасность предприятия и технологии защиты информации» предполагает использование академических аудиторий, соответствующих действующим санитарным и противопожарным правилам и нормам.

Прочее: рабочее место преподавателя, оснащенное компьютером с доступом в Интернет.

Программное обеспечение:

Функциональное назначение	Бесплатное программное обеспечение	Ссылки
Офисный пакет	Libre Office 6.3.1	https://www.libreoffice.org/ https://ru.wikipedia.org/wiki/LibreOffice

Операционная система	UBUNTU 19.04	https://ubuntu.com/ https://ru.wikipedia.org/wiki/Ubuntu
Браузер	Firefox Mozilla	http://www.mozilla.org/ru/firefox/fx
Браузер	Opera	http://www.opera.com
Почтовый клиент	Mozilla Thunderbird	http://www.mozilla.org/ru/thunderbird
Файл-менеджер	Far Manager	http://www.farmanager.com/download.php
Архиватор	7Zip	http://www.7-zip.org/
Графический редактор	GIMP (GNU Image Manipulation Program)	http://www.gimp.org/ http://gimp.ru/viewpage.php?page_id=8 http://ru.wikipedia.org/wiki/GIMP
Редактор PDF	PDFCreator	http://www.pdfforge.org/pdfcreator
Аудиоплейер	VLC	http://www.videolan.org/vlc/

8. Оценочные средства по дисциплине

Паспорт
оценочных средств по учебной дисциплине
«Информационная безопасность предприятия и технологии защиты информации»

Описание уровней сформированности и критериев оценивания компетенций на этапах их формирования в ходе изучения дисциплины

Этап	Код компетенции	Уровни сформированности компетенции	Критерии оценивания компетенции
Начальный	**ОПК-2.** Способен применять современные техники и методики сбора данных, продвинутые методы их обработки и анализа, в том числе использовать интеллектуальные информационно -аналитические системы, при решении управленческих и исследовательских задач	**Пороговый**	**знать:** современные технологии обработки информации; принципы, методы и средства решения стандартных задач с учетом основных требований информационной безопасности; основные положения теории информационной безопасности на законодательном уровне;
Основной		**Базовый**	**уметь:** решать управленческие и исследовательские задачи на основе информационной и библиографической культуры с применением информационно - коммуникационных технологий и с учетом основных требований информационной безопасности; правильно выбирать и применять меры законодательного уровня для обеспечения информационной безопасности при решении стандартных задач профессиональной деятельности;
Заключительный		**Высокий**	**владеть:** навыками количественного и качественного анализа информации при принятии управленческих решений; навыками выбора и применения мер законодательного уровня информационной безопасности при решении стандартных задач профессиональной деятельности; навыками использования современных средств информационной безопасности при решении стандартных задач профессиональной деятельности

Начальный	**ПК-4.** Способен выстраивать коммуникацию и кооперацию в цифровой среде на основе использования различных цифровых средств, позволяющих во взаимодействии с другими людьми достигать поставленных целей	**Пороговый**	**знать:** приемы коммуникации и кооперации в цифровой среде для постановки операционных целей и задач подразделениям организации; виды и источники угроз безопасности информации при решении стандартных задач профессиональной деятельности; основные требования информационной безопасности при решении профессиональной деятельности;
Основной		**Базовый**	**уметь:** проводить оценку эффективности внедрения инновационных технологий в бизнес – процессы организации; определять актуальные источники угроз безопасности при решении стандартных задач профессиональной деятельности;
Заключительный		**Высокий**	**владеть:** способами формирования и построения структуры подразделений, методами осуществления изменений при построении структуры подразделений организации; навыками поиска необходимых нормативных и законодательных документов и навыками работы с ними при оформлении технической документации на различных стадиях жизненного цикла информационной системы

Перечень компетенций (элементов компетенций), формируемых в результате освоения учебной дисциплины.

№ п/п	Код компетенции	Формулировка контролируемой компетенции	Индикаторы достижений компетенции (по дисциплине)	Темы учебной дисциплины	Этапы формирования (семестр изучения)
1	**ОПК-4.**	**ОПК-2.** Способен применять современные техники и методики сбора данных, продвинутые методы их обработки и анализа, в том числе использовать интеллектуальные информационно - аналитические системы, при решении управленческих и исследовательских задач	**ОПК-2.1.** Знает современные технологии обработки информации.	***Тема 1.*** *Понятие "информационная безопасность"* ***Тема 2.*** *Система формирования режима информационной безопасности*	2
			ОПК-2.2. Умеет решать управленческие и исследовательские задачи на основе информационной и библиографической	***Тема 3.*** *Угрозы информационной безопасности предприятия* ***Тема 4*** *Механизмы*	

			культуры с применением информационно - коммуникационных технологий и с учетом основных требований информационной безопасности.	*обеспечения "информационной безопасности"* ***Тема 5.*** *Методы и приемы обеспечения информационной безопасности*	
			ОПК-2.3. Владеет навыками количественного и качественного анализа информации при принятии управленческих решений.	***Тема 4.*** *Механизмы обеспечения "информационной безопасности"* ***Тема 6.*** *Защита информации в информационных системах*	
2.	**ПК-4.**	Способен выстраивать коммуникацию и кооперацию в цифровой среде на основе использования различных цифровых средств, позволяющих во взаимодействии с другими людьми достигать поставленных целей	**ПК-4.1.** Знает приемы коммуникации и кооперации в цифровой среде для постановки операционных целей и задач подразделениям организации;	***Тема 5.*** *Методы и приемы обеспечения информационной безопасности* ***Тема 6.*** *Защита информации в информационных системах*	2
			ПК-4.2. Умеет проводить оценку эффективности внедрения инновационных технологий в бизнес – процессы организации;	***Тема 1.*** *Понятие "информационная безопасность"* ***Тема 2.*** *Система формирования режима информационной безопасности*	
			ПК-4.3. Владеет способами формирования и построения структуры подразделений, методами осуществления изменений при построении структуры подразделений организации;	***Тема 2.*** *Система формирования режима информационной безопасности* ***Тема 3.*** *Угрозы информационной безопасности предприятия* ***Тема 4.*** *Механизмы обеспечения "информационной безопасности"*	

				Тема 6. *Защита информации в информационных системах*	

Показатели и критерии оценивания компетенций, описание шкал оценивания

№ п/п	Код компетенции	Индикаторы достижений компетенции	Планируемые результаты обучения по дисциплине	Контролируемые темы учебной дисциплины	Наименование оценочного средства
1	**ОПК-2.** Способен применять современные техники и методики сбора данных, продвинутые методы их обработки и анализа, в том числе использовать интеллектуальные информационно -аналитические системы, при решении	**ОПК-2.1.** Знает современные обработки технологии информации.	**знать:** современные технологии обработки информации; принципы, методы и средства решения стандартных задач с учетом основных требований информационной безопасности; основные положения теории информационной безопасности на законодательном уровне;	***Тема 1.*** *Понятие "информационная безопасность"* ***Тема 2.*** *Система формирования режима информационной безопасности*	Фронтальный и индивидуальный опрос, Тесты, Контрольная работа, Экзамен
		ОПК-2.2. Умеет решать управленческие и исследовательские задачи на основе информационно и библиографической культуры с применением информационно - коммуникационных технологий и учетом основных требований информационной безопасности	**уметь:** решать управленческие и исследовательские задачи на основе информационной и библиографической культуры с применением информационно - коммуникационных технологий и с учетом основных требований информационной безопасности; правильно выбирать и применять меры законодательного уровня для обеспечения информационной безопасности при решении стандартных задач профессиональной деятельности;	***Тема 3.*** *Угрозы информационной безопасности предприятия* ***Тема 4*** *Механизмы обеспечения "информационной безопасности"* ***Тема 5.*** *Методы и приемы обеспечения информационной безопасности*	Фронтальный и индивидуальный опрос, Тесты, Контрольная работа, Экзамен

		ОПК-2.3. Владеет навыками количественного и качественного анализа информации при принятии управленческих решений	**владеть:** навыками количественного и качественного анализа информации при принятии управленческих решений; навыками выбора и применения мер законодательного уровня информационной безопасности при решении стандартных задач профессиональной деятельности; навыками использования современных средств информационной безопасности при решении стандартных задач профессиональной деятельности	***Тема 4.*** *Механизмы обеспечения "информационной безопасности"* ***Тема 6.*** *Защита информации в информационных системах*	Фронтальный и индивидуальный опрос, Тесты, Контрольная работа, Экзамен
2	**ПК-4.** Способен выстраивать коммуникацию и кооперацию в цифровой среде на основе использования различных цифровых средств, позволяющих во взаимодействии с другими людьми достигать поставленных целей	**ПК-4.1.** Знает приемы коммуникации и кооперации в цифровой среде для постановки операционных целей и задач подразделениям организации.	**знать:** приемы коммуникации и кооперации в цифровой среде для постановки операционных целей и задач подразделениям организации; виды и источники угроз безопасности информации при решении стандартных задач профессиональной деятельности; основные требования информационной безопасности при решении профессиональной деятельности;	***Тема 5.*** *Методы и приемы обеспечения информационной безопасности* ***Тема 6.*** *Защита информации в информационных системах*	Фронтальный и индивидуальный опрос, Тесты, Контрольная работа, Экзамен
		ПК-4.2. Умеет проводить оценку эффективности внедрения инновационных технологий в бизнес – процессы организации.	**уметь:** проводить оценку эффективности внедрения инновационных технологий в бизнес – процессы организации; определять актуальные источники угроз безопасности при решении стандартных задач профессиональной деятельности;	***Тема 1.*** *Понятие "информационная безопасность"* ***Тема 2.*** *Система формирования режима информационной безопасности*	Фронтальный и индивидуальный опрос, Тесты, Контрольная работа, Экзамен
		ПК-4.3. Владеет способами формирования и построения структуры подразделений	способами формирования и построения структуры подразделений, методами осуществления изменений при построении структуры подразделений организации; навыками поиска необходимых	***Тема 2.*** *Система формирования режима информационной безопасности* ***Тема 3.***	Фронтальный и индивидуальный опрос, Тесты, Контрольная

			нормативных и законодательных документов и навыками работы с ними при оформлении технической документации на различных стадиях жизненного цикла информационной системы	*Угрозы информационной безопасности предприятия* ***Тема 4.*** *Механизмы обеспечения "информационной безопасности"* ***Тема 6.*** *Защита информации в информационных системах*	

Вопросы для фронтальных и индивидуальных опросов:

ТЕМА 1. ПОНЯТИЕ "ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ"

1. В чем заключается проблема информационной безопасности?
2. Дайте определение понятию "информационная безопасность".
3. Какие определения информационной безопасности приводятся в "Концепции информационной безопасности сетей связи общего пользования Российской Федерации"?
4. Что понимается под "компьютерной безопасностью"?
5. Перечислите составляющие информационной безопасности.
6. Приведите определение доступности информации.
7. Приведите определение целостности информации.
8. Приведите определение конфиденциальности информации.
9. Каким образом взаимосвязаны между собой составляющие информационной безопасности?Приведите собственные примеры.

ТЕМА 2. СИСТЕМА ФОРМИРОВАНИЯ РЕЖИМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1. Перечислите основополагающие документы по информационной безопасности.
2. Понятие государственной тайны.
3. Что понимается под средствами защиты государственной тайны?
4. Основные задачи информационной безопасности в соответствии с Концепцией национальной безопасности РФ.
5. Какие категории государственных информационных ресурсов определены в Законе "Об информации, информатизации и защите информации"?
6. Какая ответственность в Уголовном кодексе РФ предусмотрена за создание, использование и распространение вредоносных программ для ЭВМ?
1. Перечислите задачи информационной безопасности общества.
2. Перечислите уровни формирования режима информационной безопасности.
3. Дайте краткую характеристику законодательно-правового уровня.
4. Какие подуровни включает программно-технический уровень?
5. Что включает административный уровень?
6. В чем особенность морально-этического подуровня?

ТЕМА 3. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

1. Перечислите классы угроз информационной безопасности.
2. Назовите причины и источники случайных воздействий на информационные системы.
3. Дайте характеристику преднамеренным угрозам.

4. Перечислите каналы несанкционированного доступа.
5. В чем особенность "упреждающей" защиты в информационных системах.
6. Характерные черты компьютерных вирусов.
7. Дайте определение программного вируса.
8. Какие трудности возникают при определении компьютерного вируса?
9. Когда появился первый вирус, который самостоятельно дописывал себя в файлы?
10. В чем особенность компьютерного вируса "Чернобыль"?
11. Какой вид вирусов наиболее распространяемый в распределенных вычислительных сетях?Почему?
12. Как обнаружить загрузочный вирус?
13. Перечислите классификационные признаки компьютерных вирусов.
14. Охарактеризуйте файловый и загрузочный вирусы.
15. В чем особенности резидентных вирусов?
16. Поясните понятия "сканирование налету" и "сканирование по запросу".
17. Перечислите виды антивирусных программ.
18. Охарактеризуйте антивирусные сканеры.
19. Принципы функционирования блокировщиков и иммунизаторов.
20. Особенности CRC-сканеров.
21. В чем состоят особенности эвристических сканеров?
22. Какие факторы определяют качество антивирусной программы?
23. Сформулируйте признаки стелс-вирусов.
24. Перечислите деструктивные возможности компьютерных вирусов.
25. Поясните самошифрование и полиморфичность как свойства компьютерных вирусов.
26. Перечислите наиболее распространенные пути заражения компьютеров вирусами.
27. Какие особенности заражения вирусами при использовании электронной почты?
28. Особенности заражения компьютеров локальных сетей.
29. Перечислите основные правила защиты от компьютерных вирусов, получаемых не извычислительных сетей.
30. Как ограничить заражение макровирусом при работе с офисными приложениями?
31. Как обнаружить резидентный вирус?
32. Характерные черты макровируса.
33. Как проверить систему на наличие макровируса?
34. Является ли наличие скрытых листов в Excel признаком заражения макровирусом?
35. Перечислите основные этапы алгоритма обнаружения вируса.

ТЕМА 4. МЕХАНИЗМЫ ОБЕСПЕЧЕНИЯ "ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ"

1. Что входит в состав криптосистемы?
2. Какие составляющие информационной безопасности могут обеспечить криптосистемы?
3. Назовите классификационные признаки методов шифрования данных.
4. Поясните механизм шифрования "налету".
5. Как реализуется симметричный метод шифрования?
6. Как реализуется асимметричный метод шифрования?
7. Что понимается под ключом криптосистемы?
8. Какие методы шифрования используются в вычислительных сетях?
9. Что такое электронная цифровая подпись?
10. Какой метод шифрования используется в электронной цифровой подписи?
11. Чем определяется надежность криптосистемы?
12. Перечислите известные методы разграничения доступа.
13. В чем заключается разграничение доступа по спискам?
14. Как используется матрица разграничения доступа?
15. Опишите механизм разграничения доступа по уровням секретности и категориям.
16. Какие методы управления доступа предусмотрены в руководящих документах Гостехкомиссии?
17. Поясните механизм дискретного управления доступом?
18. Сравните дискретное и мандатное управление доступом.
19. На чем основан механизм регистрации?
20. Какие события, связанные с безопасностью, подлежат регистрации?
21. Чем отличаются механизмы регистрации и аудита?
22. Дайте определение аудита событий информационной системы.
23. Что относится к средствам регистрации и аудита?
24. Что такое регистрационный журнал? Его форма.
25. Что понимается под подозрительной активностью?
26. Какие этапы предусматривают механизмы регистрации и аудита?
27. Охарактеризуйте известные методы аудита безопасности информационных систем.
28. Какие сервисы безопасности включает технология виртуальных частных сетей?
29. Назовите функции VPN-агента.
30. Каким образом технология VPN обеспечивает конфиденциальность данных?
31. Каким образом технология VPN обеспечивает целостность данных?
32. Почему при использовании технологии VPN IP-адреса внутренней сети недоступны внешней сети?
33. Что такое "туннель" и технология его создания?

34. Чем определяется политика безопасности виртуальной частной сети?

ТЕМА 5. МЕТОДЫ И ПРИЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

1. Что такое компьютерный вирус?
2. Назначение компьютерного вируса?
3. Типы вирусов.
4. Программные средства защиты – антивирусные программы (характеристика).
5. Безопасность программно-технических средств и информационных ресурсов (характеристика).
6. Программная защита от несанкционированных воздействий.
7. Криптография, криптографическая защита от несанкционированных воздействий (характеристика).
8. Что такое электронная подпись?
9. Физическая и техническая защита от несанкционированных воздействий (характеристика).
10. Воздействия на здания, помещения, личную безопасность пользователя и обслуживающий персонал.
11. Технические возможности и мероприятия по обеспечению сохранности людей, зданий, помещений, программно-технических средств и информации (характеристика).
12. Охрана объектов с целью ограничения свободного доступа, смарткарты и др. (характеристика).

ТЕМА 6. ЗАЩИТА ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

1. Что такое защита информации в информационных системах
2. Защита ПК от несанкционированного доступа
3. Опознавание (аутентификация) пользователей и используемых компонентов обработки информации
4. Цели защиты информации в сетях ЭВМ
5. Понятие сервисов безопасности
6. Понятие о служебной и государственной тайне
7. Грифы ограничения доступа
8. Симметрическое и ассиметричное шифрование

Критерии и шкала оценивания по оценочному средству «фронтальный и индивидуальный опрос»

Шкала оценивания (интервал баллов)	Критерий оценивания
отлично (5)	Студент глубоко и в полном объёме владеет программным материалом. Грамотно, исчерпывающе и логично его излагает в устной или письменной форме. При этом знает рекомендованную литературу, проявляет творческий подход в ответах на вопросы и правильно обосновывает принятые решения, хорошо владеет умениями и навыками при выполнении практических задач.
хорошо (4)	Студент знает программный материал, грамотно и по сути излагает его в устной или письменной форме, допуская незначительные неточности в утверждениях, трактовках, определениях и категориях или незначительное количество ошибок. При этом владеет необходимыми умениями и навыками при выполнении практических задач.
удовлетворительно (3)	Студент знает только основной программный материал, допускает неточности, недостаточно чёткие формулировки, непоследовательность в ответах, излагаемых в устной или письменной форме. При этом недостаточно владеет умениями и навыками при выполнении практических задач. Допускает до 30% ошибок в излагаемых ответах.
неудовлетворительно (2)	Студент не знает значительной части программного материала. При этом допускает принципиальные ошибки в доказательствах, в трактовке понятий и категорий, проявляет низкую культуру знаний, не владеет основными умениями и навыками при выполнении практических задач. Студент отказывается от ответов на дополнительные вопросы

1. Типовые тестовые задания

(пороговый уровень)

1. Совокупность свойств, обусловливающих пригодность информации удовлетворять определенные потребности в соответствии с ее назначением, называется

1. актуальностью информации
2. доступностью
3. качеством информации
4. целостностью

2. Согласно «Оранжевой книге» минимальную защиту имеет группа критериев

1. C
2. A
3. B
4. D

3. Организационные требования к системе защиты

1. управленческие и идентификационные
2. административные и аппаратурные

3. административные и процедурные
4. аппаратурные и физические

4. Основу политики безопасности составляет

1. программное обеспечение
2. управление риском
3. способ управления доступом
4. выбор каналов связи

5. **Соответствие средств безопасности решаемым задачам характеризует**

1. эффективность
2. корректность
3. адекватность
4. унификация

1. С точки зрения ФСТЭК основной задачей средств безопасности является обеспечение сохранности информации

1. защиты от НСД
2. простоты реализации
3. надежности функционирования

2. Согласно «Европейским критериям» формальное описание функций безопасности требуется на уровне

1. E5
2. E7
3. E4
4. E6

3. Проверка подлинности субъекта по предъявленному им идентификатору для принятия решения о предоставлении ему доступа к ресурсам системы — это

1. аудит
2. аутентификация
3. авторизация
4. идентификация

4. Согласно «Оранжевой книге» уникальные идентификаторы должны иметь

1. наиболее важные субъекты
2. наиболее важные объекты
3. все субъекты
4. все объекты

5. Соответствие средств безопасности решаемым задачам характеризует

1. эффективность
2. корректность
3. адекватность
4. унификация

6. Нормативный документ, регламентирующий все аспекты

безопасности продукта информационных технологий, называется

1. системой защиты
2. стандартом безопасности
3. профилем безопасности
4. профилем защиты

7. Для решения проблемы правильности выбора и надежности функционирования средств защиты в «европейских критериях» вводится понятие

1. унификации средств защиты
2. надежности защиты информации
3. адекватности средств защиты
4. оптимизации средств защиты

1. Организационные требования к системе защиты

1. управленческие и идентификационные
2. административные и аппаратурные
3. административные и процедурные
4. аппаратурные и физические

2. Основу политики безопасности составляет

1. программное обеспечение
2. управление риском
3. способ управления доступом
4. выбор каналов связи

3. Абстрактное описание системы, без связи с ее реализацией, дает модель политики безопасности

1. Лендвера
2. С полным перекрытием
3. Белла-ЛаПадула
4. На основе анализа угроз

4. Из перечисленного услуга защиты целостности доступна на уровнях: 1) сетевом; 2) транспортном; 3) сеансовом; 4) канальном; 5) прикладном; 6) физическом

1. 1, 2, 5
2. 1, 3, 5
3. 1, 2, 3
4. 4, 5, 6

5. Присвоение субъектам и объектам доступа уникального номера, шифра, ключа и

т.п. с целью получения доступа к информации — это

1. идентификация
2. аудит
3. авторизация
4. аутентификация

6. Из перечисленного типами услуг аутентификации являются:

1) идентификация;
2) достоверность происхождения данных;
3) достоверность объектов коммуникации;
4) причастность;

1. 3, 4
2. 1, 4
3. 2, 3
4. 1, 2

7. Как предотвращением неавторизованного использования ресурсов определена услуга защиты

1. аутентификация
2. причастность
3. контроль доступа
4. целостность

8. Пользовательское управление данными реализуется на уровне модели взаимодействия открытых систем

представления данных

1. канальном
2. сеансовом
3. прикладном

1. Наукой, изучающей математические методы защиты информации путем ее преобразования, является

1. криптоанализ
2. криптология
3. стеганография
4. криптография

2. Конечное множество используемых для кодирования информации знаков называется

1. шифром
2. кодом
3. алфавитом
4. ключом

3. Математические методы нарушения конфиденциальности и аутентичности информации без знания ключей объединяет

1. криптология
2. стеганография
3. криптоанализ
4. криптография

4. Обеспечением скрытности информации в информационных массивах занимается

1. криптография
2. криптоанализкриптология
3. стеганография

4. Два ключа используются в криптосистемах
1. с открытым ключом
2. с закрытым ключом
3. двойного шифрования
4. симметричных

6. Главным параметром криптосистемы является показатель
1. безошибочности шифрования
2. скорости шифрования
3. криптостойкости
4. надежности функционирования

7. Длина исходного ключа в ГОСТ 28147-89 (бит)
1. 128
2. 256
3. 64

8. Основной целью системы брандмауэра является управление доступом
1. к архивам
2. внутри защищаемой сети
3. к секретной информации
4. к защищаемой сети

9. Маршрутизаторы с фильтрацией пакетов осуществляют управление доступом методом проверки
адресов отправителя и получателя
1. содержания сообщений
2. электронной подписи
3. структуры данных

10. Из перечисленного система брандмауэра может быть: 1) репитором; 2) маршрутизатором; 3) ПК; 4) хостом; 5) ресивером
1. 3, 4, 5
2. 2, 3, 4
3. 1, 4, 5
4. 1, 2, 3

1. Программа, которая может размножаться, присоединяя свой код к другой программе,называется
Выберите один ответ.
a. Компилятор
b. Интернет-черви
c. Вирус

2. Величиной (размером) ущерба (вреда), ожидаемого в результате несанкционированного доступа к информации или нарушения доступности информационной системы, называетсяВыберите один ответ.

a. Воздействием (влиянием)
b. Потерей
c. Силой

3. Код, способный самостоятельно, то есть без внедрения в другие программы, вызвать распространение своих копий по информационной системе и их выполнение, называетсяВыберите один ответ.

a. Троянской программой
b. Червем
c. Вирусом

4. Уровень риска, который считается доступным для достижения желаемого результата,называется

Выберите один ответ.

a. Устойчивостью
b. Терпимостью по отношению к риску
c. Независимостью

5. Компьютер с одним процессором в каждый конкретный момент времени может выполнятькоманд

Выберите один ответ.

a. Две
b. Одну
c. Сколько зададут

6. Алгоритмы реального времени, заранее назначающие каждому процессу фиксированныйприоритет, после чего выполняющие приоритетное планирование с переключениями,

называются:

Выберите один ответ.

a. Статическими алгоритмами
b. Алгоритмы RMS
c. Динамическими алгоритмами

7. Системные файлы, обеспечивающие поддержку структур файловой системы, называются:Выберите один ответ.

a. Каталоги
b. Символьные файлы
c. Регулярные файлы

8. Коды, обладающие способностью к распространению (возможно, с изменениями) путемвнедрения в другие программы, называются

Выберите один ответ.

a. Вирусами
b. Руткитами
c. Червями

9. Требованием к информационной системе, являющимся следствием действующего законодательства, миссии и потребностей организации,

называется:

Выберите один ответ.

a. Правилами безопасности
b. Требованием безопасности
c. Мерами безопасности

10. Процессом идентификации рисков применительно к безопасности информационной системы, определения вероятности их осуществления и потенциального воздействия, а также дополнительный контрмер, ослабляющий (уменьшающий) это воздействие, называется:

Выберите один ответ.

a. Управление риском
b. Предупреждением рисков
c. Анализом рисков

8 .Компьютерная система, в которой два или более центральных процессоров делят полныйдоступ к общей оперативной памяти, называется

Выберите один ответ.

a. Мультипроцессоры типа «хозяин-подчиненный»
b. Симметричный мультипроцессор
c. Мультипроцессор с общей памятью

Методические рекомендации:

При использовании формы текущего контроля «Тестирование» студентам могут быть предложены задания на бумажном носителе.

Критерии и шкала оценивания по оценочному средству «Тесты»

Шкала оценивания (интервал баллов)	Критерий оценивания
5	Тесты выполнены на высоком уровне (правильные ответы даны на 90-100% тестов)
4	Тесты выполнены на среднем уровне (правильные ответы даны на 75-89% тестов)
3	Тесты выполнены на низком уровне (правильные ответы даны на 50-74% тестов)
2	Тесты выполнены на неудовлетворительном уровне (правильные ответы даны менее чем на 50% тестов)

Тематика контрольных работ:

(базовый уровень)

2. Информационные ресурсы, подлежащие защите в сфере финансовой деятельности.

3. Классификация угроз информационной безопасности и их

сравнительный анализ.

4. Информационная безопасность в современных условиях хозяйствования. Общегосударственные цели, задачи и методы обеспечения информационной безопасности.

5. Понятия о видах вирусов. Классификация вирусов и угрозы для информационной инфраструктуры хозяйствующих субъектов.

6. Вида возможных нарушений информационной безопасности в сфере финансовой деятельности.

7. Отечественные и международные стандарты обеспечения информационной безопасности.

8. Особенности современной нормативно-правовой и методологической базы обеспечения информационной безопасности.

9. Основные нормативные руководящие документы, касающиеся конфиденциальной информации и государственной тайны, нормативно-справочные документы по обеспечению информационной безопасности применяемые в финансовой деятельности.

10. Общие критерии оценки безопасности информационных систем и технологий ГОСТ 15408, как основа определения требований к обеспечению информационной безопасности.

11. Место информационной безопасности экономических систем в национальной безопасности страны.

12. Цели и задачи обеспечения национальной безопасности. Система целеполагания в структуре государственного и муниципального управления при обеспечении информационной безопасности.

13. Основные положения концепции информационной безопасности. Сравнительная таблица.

14. Государственные информационные ресурсы, подлежащие защите в сфере финансовой деятельности.

15. Взаимосвязь государственных и коммерческих информационных ресурсов (конфиденциальной информации и государственной тайны).

16. Модели безопасности, и их применение.

17. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование. Оценка системы защиты информации.

18. Оценка эффективности средств и механизмов обеспечения информационной безопасности.

19. Методы анализа способов нарушений информационной безопасности.

20. Программно-аппаратные комплексы криптографической защиты, их характеристики и особенности применения. Сравнительная таблица.

21. Нормативно-правовая база криптографической защиты.

22. ЭЦП и особенности работы в системах государственного и муниципального управления.

Критерии и шкала оценивания по оценочному средству «Контрольная работа»

Шкала оценивания (интервал баллов)	Критерий оценивания
5	Контрольная работа выполнена на высоком уровне (правильные ответы даны на 90-100% вопросов/задач)
4	Контрольная работа выполнена на среднем уровне (правильные ответы даны на 75-89% вопросов/задач)
3	Контрольная работа выполнена на низком уровне (правильные ответы даны на 50-74% вопросов/задач)
2	Контрольная работа выполнена на неудовлетворительном уровне (правильные ответы даны менее чем на 50%)

Оценочные средства аттестации (экзамен)

Примерный перечень вопросов для подготовки к экзамену:

1. Понятие информационной безопасности и особенности ее обеспечения.
2. Основные составляющие информационной безопасности.
3. Основы государственной политики обеспечения информационной безопасности Российской Федерации и правовые акты и законы.
4. Законодательный уровень информационной безопасности и его важность.
5. Роль и место информационной войны в мире.
6. Средства ведения электронных информационных войн.
7. Вопросы защиты информации как составляющая общей проблемы обеспечения информационной безопасности.
8. Обзор зарубежного законодательства в области информационной безопасности.
9. Основные принципы обеспечения информационной безопасности.
10. Основные уровни информационной безопасности.
11. Обобщенная модель угроз. Внешние и внутренние угрозы.
12. Классификация угроз.
13. Стандарты обеспечения информационной безопасности.
14. Спецификации информационной безопасности.
15. Механизмы информационной безопасности.
16. Классы информационной безопасности.
17. Характеристики возможных угроз. Объекты возможных угроз. Видывозможных угроз.
18. Меры и средства защиты от угроз.
19. Меры противодействия внешним угрозам.
20. Меры противодействия внутренним угрозам.

21. Общие требования к комплексу защиты информации.
22. Общие требования к программно-техническим средствам защиты информации.
23. Угрозы информации: угрозы секретности, угрозы целостности.
24. Управление рисками информационной безопасности.
25. Политика безопасности.
26. Классификация систем защиты.
27. Роль стандартов информационной безопасности.
28. Административный уровень информационной безопасности.
29. Процедурный уровень информационной безопасности.
30. Аппаратно-программные средства защиты информации, классификацияи их применение.
31. Основные этапы реализации информационной безопасности.
32. Информационная безопасность распределенных систем.
33. Сетевые сервисы и механизмы безопасности, администрирование средств безопасности.

Критерии и шкала оценивания по оценочному средству «Экзамен»

Шкала оценивания	Характеристика знания предмета и ответов
отлично	Студент глубоко и в полном объеме владеет программным материалом. Грамотно, исчерпывающе и логично его излагает в устной или письменной форме. При этом знает рекомендованную литературу, проявляет творческий подход в ответах на вопросы и правильно обосновывает принятые решения, хорошо владеет умениями и навыками при выполнении практических задач.
хорошо	Студент знает программный материал, грамотно и по сути излагает его в устной или письменной форме, допуская незначительные неточности в утверждениях, трактовках, определениях и категориях или незначительное количество ошибок. При этом владеет необходимыми умениями и навыками при выполнении практических задач.
удовлетворительно	Студент знает только основной программный материал, допускает неточности, недостаточно четкие формулировки, непоследовательность в ответах, излагаемых в устной или письменной форме. При этом недостаточно владеет умениями и навыками при выполнении практических задач. Допускает до 30% ошибок в излагаемых ответах.
не удовлетворительно	Студент не знает значительной части программного материала. При этом допускает принципиальные ошибки в доказательствах, в трактовке понятий и категорий, проявляет низкую культуру знаний, не владеет основными умениями и навыками при выполнении практических задач. Студент отказывается от ответов на дополнительные вопросы.

Форма листа изменений и дополнений, внесенных в ФОС

Лист изменений и дополнений

№ п/п	Виды дополнений и изменений	Дата и номер протокола заседания кафедры (кафедр), на котором были рассмотрены и одобрены изменения и дополнения	Подпись (с расшифровкой) заведующего кафедрой (заведующих кафедрами)