Федеральное государственное бюджетное образовательное учреждение высшего образования
«ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ ДВАЖДЫ ГЕРОЯ СОВЕТСКОГО СОЮЗА, ЛЕТЧИКА-КОСМОНАВТА А.А. ЛЕОНОВА»

Троицкий Александр Витальевич

Подписано цифровой подписью: Троицкий Александр Витальевич

«УТВЕРЖДАЮ»
И.о. проректора
_____ А.В. Троицкий
«___»_____2023 г.

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РАБОЧАЯ ПРОГРАММА
ДИСЦИПЛИНЫ (МОДУЛЯ)

Б.1.О.15.04 «НОРМАТИВНЫЕ АКТЫ И СТАНДАРТЫ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Направление подготовки: 10.03.01 Информационная безопасность

Профиль: Организация и технологии защиты информации

Уровень высшего образования: бакалавриат

Форма обучения: очная, очно-заочная

Королев
2023

Рабочая программа является составной частью основной профессиональной образовательной программы и проходит рецензирование со стороны работодателей в составе основной профессиональной образовательной программы. Рабочая программа актуализируется и корректируется ежегодно.

Автор: Сухотерин А.И. Рабочая программа дисциплины: Нормативные акты и стандарты по информационной безопасности. – Королев МО: «Технологический университет», 2023.

Рецензент: **Соляной В.Н.**

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки бакалавров 10.03.01 «Информационная безопасность» и Учебного плана, утвержденного Ученым советом Университета. Протокол № 9 от 11.04.2023 года.

Рабочая программа рассмотрена и одобрена на заседании кафедры:

Заведующий кафедрой (ФИО, ученая степень, звание, подпись)	к.в.н., доцент Соляной В.Н.			
Год утверждения (переутверждения)	2023	2024	2025	2026
Номер и дата протокола заседания кафедры	№8 от 29.03.2023			

Рабочая программа согласована:

Руководитель ОПОП ВО Сухотерин А.И.

Рабочая программа рекомендована на заседании УМС:

Год утверждения (переутверждения)	2023	2024	2025	2026
Номер и дата протокола заседания УМС	№5 от 11.04.2023			

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ОПОП

Целью изучения дисциплины является:

1. Формирование у студентов специализированной базы знаний по фундаментальным проблемам информационной безопасности в условиях становления современного информационного общества.
2. Использование организационно-правовых механизмов обеспечения конституционных прав и свобод граждан в информационной сфере и регламентирующих создание и использование защищённых информационных технологий.
3. Получение первичных навыков в применении защищённых технологий при обеспечении информационной безопасности различных объектов.

В процессе обучения студент приобретает и совершенствует следующие компетенции.

ДОПК-2. Способен формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы;

ДОПК-3. Способен разработать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности;

ДОПК-4. Способен проводить аудит защищенности объекта информатизации в соответствии с нормативными документами;

Основными **задачами** дисциплины являются:

1. Ознакомление студентов с процессами стандартизации компьютерных информационных систем с точки зрения информационной безопасности;
2. Ознакомление студентов с нормативно-правовым обеспечением компьютерных информационных систем по защите информации;
3. Формирование у студентов способности самостоятельно проводить классификацию автоматизированных систем и средств защиты информации по требованиям безопасности;
4. Формирование студентами предложений по совершенствованию, модернизации, унификации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами.

Показатель освоения компетенции отражают следующие индикаторы:

Необходимые знания:

- знает подходы к построению подсистем фиксации и реагирования на инциденты информационной безопасности
- знает принципы разработки организационных и технических мер по сбору, анализу и мониторингу событий безопасности
- знает как проводится анализ журналов событий средств защиты информации
- знает основные этапы расследования компьютерных преступлений в соответствии с нормативными требованиями
- знает руководящие документы в области классификации современных информационных систем и средств вычислительной и техники
- знает основы нормативно-правовых актов в области защиты информации конфиденциального характера
- знает как формируется организационно-распорядительная и эксплуатационная документация по обеспечению безопасности информационных систем
- знает государственные нормативные документы в области организации проведения и сопровождения аттестации объекта информатизации
- знает отечественные и зарубежные стандарты в области информационной безопасности
- знает как разрабатывать технические задания на создание подсистем информационной безопасности открытых информационных систем
- знает правовые нормы, инструкции и стандарты в области организации документооборота
- знает правовые основы организации защиты государственной тайны и конфиденциальной информации
- знает стандарты и критерии в области аудита ИБ
- знает требования законодательства по обеспечению безопасности персональных данных
- знает как составляются политики информационной безопасности в информационной системе персональных данных
- знает принципы организации процесса аудита
- знает теоретическую базу разработки политик безопасности
- знает теоретическую базу и средства для проведения мониторинга защищенности информационной системы
- знает принципы администрирования подсистем информационной безопасности
- знает порядок аттестации объектов информатизации
- знает порядок проведения сертификационных испытаний средств защиты информации

Необходимые умения:

- умеет анализировать эффективность применения мер по обеспечению ЗИ и разрабатывать предложения по совершенствованию структуры мер и повышению эффективности.
- умеет реагировать на инциденты информационной безопасности
- умеет сопоставлять основные структурно-функциональные характеристики информационных систем с требованиями руководящих документов
- умеет классифицировать информацию и автоматизированные системы, определять основные требования к ее защите

- умеет организовывать проведение и сопровождать аттестацию объекта информатизации в соответствии с требованиями нормативных документов
- умеет разрабатывать инструкции по организации защищённого документооборота и контролировать их исполнение
- умеет формировать требования к системам защиты информации в информационных системах персональных данных с учетом специфики их эксплуатации в различных сферах жизнедеятельности
- умеет определять объекты аудита, критерии и область их действия
- умеет применять инструментальные средства мониторинга и аудита безопасности
- умеет составлять программу аудита ИБ
- умеет разрабатывать методики анализа рисков
- умеет собирать и анализировать свидетельства аудита
- умеет формализовать задачи анализа безопасности информационных систем

Трудовые действия:

- владеет навыками классификации информационных систем и средств вычислительной техники по требованиям регуляторов ИБ
- владеет навыками сравнения и анализа существующих средств защиты информации
- владеет навыками нахождения наиболее подходящего решения применительно к заданным характеристикам информационной системы
- владеет навыками работы с нормативно-правовыми актами, навыками ориентации в них и поиска необходимой информации
- владеет навыками внедрения и контроля исполнения требования локальных нормативных документов по обеспечению ИБ
- владеет навыками проведения лицензирования в области защиты информации
- владеет навыками работы с нормативно-правовыми актами
- владеет навыками составления отчётов по результатам выполненного аудита
- владеет навыками проведения аудита ИБ со сбором данных
- владеет навыками по формулированию выводов и заключения по полученным результатам
- владеет навыками выбора и обоснования критериев оценки защищенности открытых информационных систем

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Нормативные акты и стандарты по информационной безопасности» относится к обязательной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Организационное и

правовое обеспечение информационной безопасности», «Математическая логика и теория алгоритмов» и компетенциях: ОПК-1,3,5,6,8.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Экономика информационной безопасности», «Информационно-аналитическая деятельность по обеспечению комплексной безопасности», «Лицензирование и сертификация в области защиты информации», «Аттестация в области защиты информации», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

3. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины для студентов очной и очно-заочной формы составляет 4 зачетные единицы, 144 часа.

Таблица1

Виды занятий	Всего часов	Семестр 7	Семестр 8	Семестр …	Семестр …
Общая трудоемкость	108	108	108		
ОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	48	48			
Лекции (Л)	16	16			
Практические занятия (ПЗ)	16	16			
Лабораторные работы (ЛР)	**16**	**-16**			
Самостоятельная работа	50	50			
Другие виды контактной работы	**10**	**10**			
Практическая подготовка	нет	-нет			
Курсовые работы (проекты)	-	-			
Расчетно-графические работы	-	-			
Контрольная работа, домашнее задание	+	+			
Текущий контроль знаний (7 - 8, 15 - 16 недели) -2ч	Т1;Т2	Т1;Т2			
Вид итогового контроля	Экзамен	Экзпмен			
ОЧНО - ЗАОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	24		24		
Лекции (Л)	12		12		
Практические занятия (ПЗ)	8		8		
Лабораторные работы (ЛР)	4		4		
Самостоятельная работа	82		82		
Другие виды контактной работы	**10**		10		
Практическая подготовка	Нет		Нет		
Курсовые работы (проекты)	-		-		

Расчетно-графические работы	-		-		
Контрольная работа, домашнее задание	+		+		
Вид итогового контроля	Экзамен		Экзамен		

Под другими видами контактной работы понимается: групповые и индивидуальные консультации, тестирование

4. Содержание дисциплины

Таблица 2

Наименование тем	Лекции, час. Очно/очно-заочное	Практические занятия, Час. Очно/очно-заочное	Занятия в интерактивной форме, час	Код компетенций
Тема 1. Введение в дисциплину. Общие сведения о стандартах в области информационной безопасности	1/2	1/1	1/1	ДОПК-2
Тема 2. Международные стандарты информационной безопасности	3/2	3/1	1/1	ДОПК-2
Тема 3. Отечественные стандарты информационной безопасности	3/2	3/1	1/2	ДОПК-3
Тема 4. Критерии оценки доверенных компьютерных систем («Оранжевая книга»)	3/2	3/1	3/2	ДОПК-4
Тема 5. Руководящие	3/2	3/2	3/2	ДОПК-4

документы Гостехкомиссии России (ФСТЭК).				
Тема 6. Общие критерии	3/2	3/2	3/2	ДОПК-4
Итого:	16/12	16/8	12/10	

4.2. Содержание тем дисциплины

Тема 1. Введение в дисциплину

Общие сведения о стандартах в области информационной безопасности.

Понятие стандарта в области информационной безопасности (ИБ). Обоснование необходимости использования стандартов ИБ. Классификация стандартов ИБ.

Тема 2. Международные стандарты информационной безопасности

Стандарты ISO/IEC 17799-2002 (BS 7799-2000). Стандарт ISO/IEC 27001:2005. Модель PDCA. Германский стандарт BSI. Общие критерии безопасности информационных технологий (стандарт ISO 15408-1999). Стандарты для беспроводных сетей. Стандарты в сети Internet.

Тема 3. Отечественные стандарты информационной безопасности

Нормативные документы по критериям оценки защищенности средств вычислительной техники (СВТ) и автоматизированных систем (АС). Документы, регулирующие информационную безопасность. Достоинства ГОСТ Р ИСО/МЭК 15408.

Тема 4. Критерии оценки доверенных компьютерных систем

(«Оранжевая книга»)

Назначение и структура требований. Группы классов защищенности и их характеристики.

Тема 5. Руководящие документы ФСТЭК

Основные положения концепции защиты СВТ и АС от НСД к информации. Защита от НСД к информации в СВТ и АС. Межсетевые экраны. Показатели защищенности. Классификация АС и требования по защите информации. Программное обеспечение средств защиты информации.

Тема 6. Общие критерии

Основные положения. Структура и содержание профиля защиты. Структура и содержание задания по безопасности. Функциональные требования безопасности. Требования доверия. Методы оценки. Оценочные уровни доверия.

5. Перечень учебно-методического обеспечения для самостоятельной работы по дисциплине

«Методические указания для самостоятельной работы обучающихся по освоению дисциплины» представлены в Приложении 2.

6. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

Структура фонда оценочных средств, для проведения промежуточной аттестации обучающихся по дисциплине «Нормативные акты и стандарты по информационной безопасности» приведена в Приложении 1.

7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Основная литература:

1.Ермакова, А. Ю. Методы и средства защиты компьютерной информации : учебное пособие / А. Ю. Ермакова. — Москва : РТУ МИРЭА, 2020. — 223 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/163844 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

2.Пугин, В. В. Защита информации в компьютерных информационных системах : учебное пособие / В. В. Пугин, Е. Ю. Голубничая, С. А. Лабада. — Самара : ПГУТИ, 2018. — 119 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/182299 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

3.Электронный документооборот и обеспечение безопасности стандартными средствами WINDOWS : учебное пособие / Л.М. Евдокимова, В.В. Корябкин, А.Н. Пылькин, О.Г. Швечкова. - Москва : КУРС, 2023. - 296 с. - ISBN 978-5-906923-24-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1902497 (дата обращения: 30.11.2022). – Режим доступа: по подписке.

4.Информационные технологии в документационном обеспечении управления и архивном деле : учебник для вузов / Н. Н. Кунаев, Т. В. Кондрашова, Е. В. Терентьева, А. Г. Фабричнов / под общ. ред. Н. Н. Куняева. - Москва : Логос, 2020. - 408 с. - ISBN 978-5-98704-786-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1211641 (дата обращения: 30.11.2022). – Режим доступа: по подписке.

5.Моргунов, А. В. Электронные системы документооборота : учебное пособие / А. В. Моргунов. - Новосибирск : Изд-во НГТУ, 2020. - 74 с. - ISBN 978-5-7782-4269-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/1870515 (дата обращения: 30.11.2022). – Режим доступа: по подписке.

Дополнительная литература:

6.Конфиденциальное делопроизводство и защищенный электронный документооборот : учебник / Н. Н. Куняев, А. С. Дёмушкин, Т. В. Кондрашова, А. Г. Фабричнов ; под общ. ред. Н. Н. Куняева. - 2-е изд., перераб. и доп. - Москва : Логос, 2020. - 500 с. - (Новая университетская библиотека). - ISBN 978-5-98704-711-8. - Текст : электронный. - URL:

https://znanium.com/catalog/product/1212394 (дата обращения: 30.11.2022). – Режим доступа: по подписке.
7.Раздорожный, А. А. Документирование управленческой деятельности : учеб. пособие / А.А. Раздорожный. — Москва : ИНФРА-М, 2018. — 304 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-16-011744-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/969585 (дата обращения: 30.11.2022). – Режим доступа: по подписке.
8.Информационные технологии в документационном обеспечении управления и архивном деле : учебник для вузов / Н. Н. Кунаев, Т. В. Кондрашова, Е. В. Терентьева, А. Г. Фабричнов / под общ. ред. Н. Н. Куняева. - Москва : Логос, 2020. - 408 с. - ISBN 978-5-98704-786-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1211641 (дата обращения: 30.11.2022). – Режим доступа: по подписке.

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

Интернет-ресурсы:

1. **http://eup.ru/catalog/all-all.asp** – научно-образовательный портал.
2. **http://informika.ru/** – образовательный портал.
3. **www.wikIsec.ru** - Энциклопедия информационной безопасности. – Публикации, статьи.
4. **www.biblioclub.ru** - Универсальная библиотека онлайн.
5. **www.rucont.ru** - ЭБС «Руконт».
6. **http://www.academy.it.ru/ –** академия АЙТИ.
7. **http://www.minfin.ru** - Официальный сайт Министерства финансов Российской Федерации
8. **http://www.gov.ru/** - Официальный сервер органов государственной власти Российской Федерации**.**
9. **http://www.fsb.ru/ -** Официальный сайт Федеральной Службы Безопасности
10. **http://www.fstec.ru/** - Официальный сайт Федеральной Службы по Техническому Экспортному контролю

9. Методические указания для обучающихся, по освоению дисциплины

Методические указания для обучающихся, по освоению дисциплины (модуля) приведены в Приложении 2 к настоящей рабочей программе.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

Перечень программного обеспечения: MSOffice.

Информационные справочные системы:

1.Электронные ресурсы образовательной среды Университета.
2.Информационно-справочные системы (Консультант+; Гарант).

Ресурсы информационно-образовательной среды МГОТУ:

Рабочая программа и методическое обеспечение по курсу «Нормативные акты и стандарты по информационной безопасности»

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Лекционные занятия:

- аудитория, оснащенная презентационной техникой (проектор, экран);
- комплект электронных презентаций / слайдов на темы:

Практические занятия:

- компьютерный класс с проектором для интерактивного обучения и проведения лекций в форме слайд-презентаций, оборудованный современными лицензионными программно-техническими средствами: операционная система не ниже WindowsXP; офисные программы MSOffice 7;
- рабочее место преподавателя, оснащенное компьютером с доступом в Интернет;
- рабочие места студентов, оснащенные компьютерами с доступом в Интернет.

Приложение 1

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

«НОРМАТИВНЫЕ АКТЫ И СТАНДАРТЫ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Направление подготовки: 10.03.01 Информационная безопасность

Профиль: Организация и технологии защиты информации

Уровень высшего образования: бакалавр

Форма обучения: очная, очно-заочная

Королев
2023

1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

№ п/п	Индекс компе-тенции	Содержание компетенции	Раздел дисциплины, обеспечивающий формирование компетенции	В результате изучения раздела дисциплины, обеспечивающего формирование компетенции, обучающийся приобретает:		
				Трудовые действия	Необходимые умения	Необходимые знания
1.	ДОПК-2	Способен формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы;	Темы 1, 2,3, 4, 5,6	- владеет навыками классификации информационных систем и средств вычислительной техники по требованиям регуляторов ИБ - владеет навыками сравнения и анализа существующих средств защиты информации - владеет навыками нахождения наиболее подходящего решения применительно к заданным характеристикам информационной системы - владеет навыками работы с нормативно-	- умеет анализировать эффективность применения мер по обеспечению ЗИ и разрабатывать предложения по совершенствованию структуры мер и повышению эффективности. - умеет реагировать на инциденты информационной безопасности - умеет сопоставлять основные структурно-функциональные характеристики информационных систем с требованиями	- знает подходы к построению подсистем фиксации и реагирования на инциденты информационной безопасности - знает принципы разработки организационных и технических мер по сбору, анализу и мониторингу событий безопасности - знает как проводится анализ журналов событий средств защиты информации - знает основные этапы расследования компьютерных преступлений в соответствии с нормативными требованиями - знает руководящие документы в области классификации современных информационных систем и средств

				правовыми актами, навыками ориентации в них и поиска необходимой информации	руководящих документов - умеет классифицировать информацию и автоматизированные системы, определять основные требования к ее защите	вычислительной и техники - знает основы нормативно-правовых актов в области защиты информации конфиденциального характера - знает как формируется организационно-распорядительная и эксплуатационная документация по обеспечению безопасности информационных систем
2.	ДОПК-3	Способен разработать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности	Темы 1,2,3, 4, 5,6	- владеет навыками внедрения и контроля исполнения требования локальных нормативных документов по обеспечению ИБ - владеет навыками проведения лицензирования в области защиты информации - владеет	- умеет организовывать проведение и сопровождать аттестацию объекта информатизации в соответствии с требованиями нормативных документов - умеет разрабатывать инструкции по организации	- знает государственные нормативные документы в области организации проведения и сопровождения аттестации объекта информатизации - знает отечественные и зарубежные стандарты в области информационной безопастности; - знает как разрабатывать технические задания на создание

				навыками работы с нормативно-правовыми актами	защищённого документооборота и контролировать их исполнение - умеет формировать требования к системам защиты информации в информационных системах персональных данных с учетом специфики их эксплуатации в различных сферах жизнедеятельности	подсистем информационной безопасности открытых информационных систем - знает правовые нормы, инструкции и стандарты в области организации документооборота - знает правовые основы организации защиты государственной тайны и конфиденциальной информации - знает как разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации - знает актуальные нормативно-правовые акты и методические документы в области обеспечения информационной

						безопасности персональных данных - знает правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны в соответствии с доктриной ИБ РФ
3.	ДОПК-4	Способен проводить аудит защищенности объекта информатизации в соответствии с нормативными документами	Темы 1, 2,3, 4, 5,6	- владеет навыками составления отчётов по результатам выполненного аудита - владеет навыками проведения аудита ИБ со сбором данных - владеет навыками по формулированию выводов и заключени	- умеет определять объекты аудита, критерии и область их действия - умеет применять инструментальные средства мониторинга и аудита безопасности - умеет составлять программу аудита ИБ - умеет разрабаты	- знает стандарты и критерии в области аудита ИБ - знает требования законодательства по обеспечению безопасности персональных данных - знает как составляются политики информационной безопасности в информационной системе персональных данных

				я по полученным результатам - владеет навыками выбора и обоснования критериев оценки защищенности открытых информационных систем	вать методики анализа рисков - умеет собирать и анализировать свидетельства аудита - умеет формализовать задачи анализа безопасности информационных систем	- знает принципы организации процесса аудита - знает теоретическую базу разработки политик безопасности - знает теоретическую базу и средства для проведения мониторинга защищенности информационной системы - знает принципы администрирования подсистем информационной безопасности - знает порядок аттестации объектов информатизации - знает порядок проведения сертификационных испытаний средств защиты информации

2.Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Код компетенции	*Инструмент, оценивающий сформированность компетенции*	*Этапы и показатель оценивания компетенции*	*Критерии оценивания компетенции на различных этапах формирования и шкалы оценивания*
ДОПК-2,3,4	*Доклад*	*А) полностью сформирована (компетенция освоена на высоком уровне) – 5 баллов* *Б) частично сформирована:* • *компетенция освоена на продвинутом уровне – 4 балла;* • *компетенция освоена на базовом уровне – 3 балла;* *В) не сформирована (компетенция не сформирована) – 2 и менее баллов*	*Например:* *Проводится в письменной и/или устной форме.* *Критерии оценки:* *1. Соответствие содержания доклада заявленной тематике (1 балл).* *2. Качество источников и их количество при подготовке работы (1 балл).* *3. Владение информацией и способность отвечать на вопросы аудитории (1 балл).* *4. Качество самой представленной работы (1 балл).* *5. Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл).* *Максимальная сумма баллов - 5 баллов.*
ДОПК-2,3,4	*Выполнение контрольной работы*	*А) полностью сформирована (компетенция освоена на высоком уровне) – 5 баллов* *Б) частично сформирована:* • *компетенция освоена на продвинутом уровне – 4 балла;* • *компетенция освоена на базовом уровне – 3 балла;* *В) не сформирована (компетенция не сформирована) – 2 и менее баллов*	*При определении сформированности компетенций критериями оценивания выступают методические рекомендации, разработанные по дисциплине для данного вида*

3. 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

Примерная тематика докладов в презентационной форме:

1. Предназначение стандартов информационной безопасности (ИБ), необходимость их использования.
2. Общие критерии безопасности информационных технологий (стандарт ISO 15408).
3. Взаимосвязь между общими критериями и общей методологией оценки.
4. Структура технического отчета об оценке.
5. Стандарты для беспроводных сетей.
6. Стандарты в сети Internet.
7. Отечественные стандарты безопасности информационных технологий.
8. Нормативные документы по критериям оценки защищенности средств вычислительной техники (СВТ) и автоматизированных систем (АС).
9. Документы, регулирующие информационную безопасность. Достоинства ГОСТ Р ИСО/МЭК 15408 - 2002.
10. Структура функционального класса.
11. Структура функционального семейства.
12. Общая схема представления класса.
13. Структура функционального компонента.
14. Критерии оценки доверенных компьютерных систем («Оранжевая книга»). Назначение и структура требований.
15. Группы классов защищенности и их характеристики.
16. Руководящие документы Гостехкомиссии России (ФСТЭК).
17. Межсетевые экраны. Показатели защищенности.
18. Классификация АС и требования по защите информации.
19. Программное обеспечение средств защиты информации.
20. Общие критерии. Основные положения.
21. Структура и содержание профиля защиты.
22. Структура и содержание задания по безопасности.
23. Функциональные требования безопасности.
24. Требования доверия. Методы оценки. Оценочные уровни доверия.
25. Основные положения концепции защиты СВТ и АС от НСД к информации
26. Средства вычислительной техники. Защита от НСД к информации. Показатели защищённости от НСД к информации
27. Автоматизированные системы. Защита от НСД к информации. Классификация. АС и требования по защите информации
28. ISO/IEC 17799:2005
29. ISO/IEC 27001:2005
30. BS 7799-3:2006

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

Формой контроля знаний по дисциплине «Нормативные акты и стандарты по информационной безопасности» являются две текущие аттестации в виде тестов и итоговая аттестация в виде экзамена.

Неделя текущего контроля	Вид оценочного средства	Код компетенций, оценивающий знания, умения, навыки	Содержание оценочного средства	Требования к выполнению	Срок сдачи (неделя семестра)	Критерии оценки по содержанию и качеству с указанием баллов
Проводится в сроки, установленные графиком образовательного процесса	тестирование	ДОПК-2,3,4	20-40 вопросов	Компьютерное тестирование ; время отведенное на процедуру - 30 минут	Результаты тестирования предоставляются в день проведения процедуры	***Преподаватель указывает критерии оценки данного вида контроля. Например, критерии оценки определяются процентным соотношением. Неявка – 0. Неудовлетворительно – менее 50% правильных ответов Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%.***
Проводится в сроки, установленные графиком образовательного процесса	тестирование	ДОПК-2,3,4	20 вопросов	Компьютерное тестирование; время отведенное на процедуру – 30 минут	Результаты тестирования предоставляются в день проведения процедуры	***Преподаватель указывает критерии оценки данного вида контроля. Например, критерии оценки определяются процентным соотношением. Неявка – 0. Неудовлетворительно – менее 50% правильных ответов Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%.***
Провод	Экзамен	ДОПК-	2	Экзамен	Результат	Критерии

ится в сроки, установленные графиком образовательного процесса		2,3,4	теоретических вопроса + практическое задание	проводится в письменной форме, путем ответа на вопросы. Время, отведенное на процедуру – 30 минут.	ы предоставляются в день проведения зачета	оценки: «**Отлично**»: • знание основных понятий предмета; • умение использовать и применять полученные знания на практике; • работа на практических занятиях; • знание основных научных теорий, изучаемых предметов; • ответ на вопросы билета. «**Хорошо**»: • знание основных понятий предмета; • умение использовать и применять полученные знания на практике; • работа на практических занятиях; • знание основных научных теорий, изучаемых предметов; • ответы на вопросы билета • неправильно решено практическое задание «У**довлетвори-**

						тельно»: • демонстрирует частичные знания по темам дисциплин; • незнание неумение использовать и применять полученные знания на практике; • не работал на практических занятиях; «**Неудовлетвори-тельно**»: • демонстрирует частичные знания по темам дисциплин; • незнание основных понятий предмета; • неумение использовать и применять полученные знания на практике; • не работал на практических занятиях; • не отвечает на вопросы.

Примерное содержание тестов для текущей аттестации:

ЗАДАНИЕ НА ВЫБОР ОДНОГО ПРАВИЛЬНОГО ВАРИАНТА ОТВЕТА

1. Чем вызвана необходимость решения задачи стандартизации ИТ ?

– правовыми аспектами

- совершенствованием процесса производства ИТ

– обеспечением совместимости продуктов и систем

2. Какие стандарты ИБ относят к спецификации?

– общие критерии

– управленческие стандарты

– руководящие документы ФСТЭК

3. Какой стандарт является обязательным для применения в СЗИ ?

– ГОСТ 28147-89

– ГОСТ Р ИСО/МЭК 15408-2002

– ISO 17799-2005

4. Какие стандарты применяются при проведении сертификации средств защиты, предназначенных для работы с информацией, относящейся к гостайне ?

– руководящие документы ФСТЭК

– ГОСТ 3411-2004

– ISO 27001-2005

5. Чем должна определяться возможность доступа субъектов к объектам?

– на основании распоряжений руководства организации

– на основании их идентификации и набора правил управления доступом

– на основании уровня конфиденциальности информации

6. От чего должны быть защищены все средства защиты ?

– сбоев в работе программного обеспечения

– от вирусов

– от несанкционированного вмешательства и отключения

7. Требуемый уровень защищённости системы возрастает?

– от группы **A** к группе **D**

– от группы **D** к группе **A**

– с уменьшением номера класса в пределах одной группы

8. Что понимается под несанкционированным доступом (НСД) ?

– доступ к информации, нарушающий установленные правила разграничения

– доступ к информации с использованием специальных программ

– доступ к информации с использованием нештатных СВТ

9. Какой субъект рассматривается в качестве нарушителя согласно РД ФСТЭК?

– не имеющий доступ к работе со штатными средствами АС и СВТ

– имеющий доступ к работе со штатными средствами АС и СВТ

– любой субъект, нарушающий правила разграничения доступа

10. Какой документ оформляется по результатам успешных испытаний СВТ и АС ?

– сертификат

– протокол проведения испытаний

– экспертное заключение

11. Какое количество групп и классов защищённости СВТ от НСД устанавливается в соответствии с РД ФСТЭК ?

– 8 классов защищённости, разбитые на 2 группы

– 3 группы, разбитые на 7 классов защищённости

– 7 классов защищённости, разбитые на 4 группы

12. Какое количество групп и классов защищённости АС от НСД устанавливается в соответствии с РД ФСТЭК ?

– 9 классов защищённости, разбитые на 3 группы

– 7 классов защищённости, разбитые на 5 групп

– 4 группы, разбитые на 6 классов защищённости

13. С помощью чего осуществляется реализация СУИБ ?

– на основании применения необходимых механизмов безопасности

– на основании политики безопасности

– на основании внедрения 4-х фазной модели PDCA

14. В каком международном стандарте описывается процесс оценки рисков?

– в Германском стандарте BSI

– в Британском стандарте BS 7799-3:2006

– в стандарте ISO/IEC 15408-1999

15. Какой протокол используются для управления доступом в беспроводную сеть ?

– IPSec

– SSL

– MAC

16. Какой метод используется в качестве базовой технологии в стандарте IEEE 802.11b ?

– метод частотного мультиплексирования OFDM

– метод распределённого спектра с прямой последовательностью DSSS

– алгоритм RC4

17. Что представляет собой протокол WEP ?

– протокол безопасных электронных транзакций

– протокол расширенной аутентификации

– протокол шифрования

18. Что такое функциональный элемент ?

– имя класса

– характеристика семейства

– наименьшее функциональное требование безопасности

19. Что обозначает запись *FDP_IFF A.2* ?

– спецификацию продукта

– идентификационный код

– краткую форму имени функционального элемента

20. Что определяет краткая спецификация объекта ?

– структуру и содержание задания по безопасности

– профиль защиты оцениваемого объекта

– отображение требований безопасности для объекта оценки

21. Что такое «характеристика семейства» ?

– оценка продукта или системы

– каталог функциональных требований

– описание функционального семейства, в котором излагаются его цели безопасности и общее описание функциональных требований

22. Сколько семейств доверия содержит класс доверия?

– не более шести

– по меньшей мере, одно семейство доверия

– не менее трёх

23. Сколько оценочных уровней доверия определено ГОСТ Р ИСО/МЭК 15408-2002?

– 6

– 4

– семь

Типовые вопросы, выносимые на экзамен

1. Предназначение стандартов информационной безопасности (ИБ), необходимость их использования.
2. Классификация стандартов ИБ.
3. Международные стандарты ИБ.
4. Стандарт ISO/IEC 27001:2005. Модель PDCA.
5. Стандарт ISO/IEC 17799:2002 (BS7799:2000). Модель управления рисками.
6. Германский стандарт BSI.
7. Общие критерии безопасности информационных технологий (стандарт ISO 15408).
8. Взаимосвязь между общими критериями и общей методологией оценки.
9. Структура технического отчета об оценке.
10. Стандарты для беспроводных сетей.
11. Стандарты в сети Internet.
12. Отечественные стандарты безопасности информационных технологий.
13. Нормативные документы по критериям оценки защищенности средств вычислительной техники (СВТ) и автоматизированных систем (АС).
14. Документы, регулирующие информационную безопасность. Достоинства ГОСТ Р ИСО/МЭК 15408 - 2002.
15. Структура функционального класса.
16. Структура функционального семейства.
17. Общая схема представления класса.
18. Структура функционального компонента.
19. Критерии оценки доверенных компьютерных систем («Оранжевая книга»). Назначение и структура требований.

20. Группы классов защищенности и их характеристики.

21. Руководящие документы Гостехкомиссии России (ФСТЭК).

22. Несанкционированный доступ (НСД). Способы НСД. Классификация нарушителей.

23. Межсетевые экраны. Показатели защищенности.

24. Классификация АС и требования по защите информации.

25. Программное обеспечение средств защиты информации.

26. Общие критерии. Основные положения.

27. Структура и содержание профиля защиты.

28. Структура и содержание задания по безопасности.

29. Функциональные требования безопасности.

30. Требования доверия. Методы оценки. Оценочные уровни доверия.

**Итоговое начисление баллов по дисциплине осуществляется в соответствии с разработанной и внедренной балльно-рейтинговой системой контроля и оценивания уровня знаний и внеучебной созидательной активности обучающихся.*

Приложение 2

Методические указания для обучающихся по освоению дисциплины (модуля)

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

«НОРМАТИВНЫЕ АКТЫ И СТАНДАРТЫ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Направление подготовки: 10.03.01 «Информационная безопасность»

Профиль: Организация и технологии защиты информации

Уровень высшего образования: бакалавр

Форма обучения: очная, очно-заочная

Королев
2023

1. Общие положения

Целями изучения дисциплины является:

– Формирование у студентов специализированной базы знаний по фундаментальным проблемам информационной безопасности в условиях становления современного информационного общества.

– Использование организационно-правовых механизмов обеспечения конституционных прав и свобод граждан в информационной сфере и регламентирующих создание и использование защищённых информационных технологий.

– Получение первичных навыков в применении защищённых технологий при обеспечении информационной безопасности различных объектов.

Задачами дисциплины является:

1. Ознакомление студентов с процессами стандартизации компьютерных информационных систем с точки зрения информационной безопасности;
2. Ознакомление студентов с нормативно-правовым обеспечением компьютерных информационных систем по защите информации;
3. Формирование у студентов способности самостоятельно проводить классификацию автоматизированных систем и средств защиты информации по требованиям безопасности;
4. Формирование студентами предложений по совершенствованию, модернизации, унификации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами.

2. Указания по проведению практических занятий

Тема 1: Введение в дисциплину. Общие сведения о стандартах в области информационной безопасности

Практическое занятие 1.

Вид практического занятия**:** ***подготовка доклада.***

Образовательные технологии: ***групповая дискуссия.***

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Ознакомиться с основными понятиями дисциплины и общими положениями о стандартах в области информационной безопасности

Основные положения темы занятия:

1. Общие сведения.

2. Классификация стандартов в области информационной безопасности.

Вопросы для обсуждения:

Основной доклад (реферат) по теме занятия.

1. Предназначение стандартов информационной безопасности (ИБ), необходимость их использования.
2. Взаимосвязь между общими критериями и общей методологией оценки.
3. Структура технического отчета об оценке.

Продолжительность занятия: 3/2 ч.

Тема 2: Международные стандарты информационной безопасности

Практическое занятие 2.

Вид практического занятия**: *подготовка доклада.***

Образовательные технологии: ***групповая дискуссия.***

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Ознакомиться с международными стандартами в области информационной безопасности

Основные положения темы занятия:

1. Перечень международных стандартов ИБ.
2. Функции международных стандартов ИБ.

Вопросы для обсуждения:

Основной доклад (реферат) по теме занятия.

1. ISO/IEC 17799:2005
2. ISO/IEC 27001:2005
3. BS 7799-3:2006

Продолжительность занятия: 3/2 ч.

Тема 3: Отечественные стандарты информационной безопасности

Практическое занятие 3.

Вид практического занятия**: *подготовка доклада.***

Образовательные технологии: ***групповая дискуссия.***

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Ознакомиться с российскими стандартами в области информационной безопасности.

Основные положения темы занятия:

1. Перечень российских стандартов ИБ.
2. Функции российских стандартов ИБ.

Вопросы для обсуждения:

Основной доклад (реферат) по теме занятия.

1.Основополагающий государственный стандарт Российской Федерации в области защиты информации.

2.Руководящие документы ФСТЭК России.

Продолжительность занятия: 3/2 ч.

Тема 4: Критерии оценки доверенных компьютерных систем («Оранжевая книга»)

Практическое занятие 4.

Вид практического занятия**: *подготовка доклада.***

Образовательные технологии: ***групповая дискуссия.***

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить базовые знания о стандарте **«Критерии оценки доверенных компьютерных систем»**.

Основные положения темы занятия:

1. Общее понятие стандарта.
2. Требования и функции «Оранжевой книги».

Вопросы для обсуждения:

Основной доклад (реферат) по теме занятия.

1. Основные положения оранжевой книги
2. Механизмы безопасности
3. Классы безопасности

Продолжительность занятия: 2/2 ч.

Тема 5: Руководящие документы Гостехкомиссии России (ФСТЭК)

Практическое занятие 5.

Вид практического занятия**: *подготовка доклада.***

Образовательные технологии: ***групповая дискуссия.***

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить представление об основных документах ФСТЭК России.

Основные положения темы занятия:

1. Ознакомиться с классификацией автоматизированных систем по уровню защищенности от несанкционированного доступа
2. Ознакомиться с классификацией межсетевых экранов по уровню защищенности от несанкционированного доступа

Вопросы для обсуждения:

Основной доклад (реферат) по теме занятия.

1. Классификация автоматизированных систем по уровню защищенности от несанкционированного доступа
2. Классификация межсетевых экранов по уровню защищенности от несанкционированного доступа

Продолжительность занятия: 4/2 ч.

Тема 6: Общие критерии безопасности информационных технологий

Практическое занятие 6.

Вид практического занятия**: *подготовка доклада.***

Образовательные технологии: ***групповая дискуссия.***

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические навыки в формировании и построении защищенной системы электронного документооборота в кредитно-финансовой организации.

Основные положения темы занятия:

1. Общее понятие стандарта
2. Требования и функции Общих критериев.

Вопросы для обсуждения:

Основной доклад (реферат) по теме занятия.

1. Основные положения Общих критериев
2. Механизмы безопасности
3. Классы безопасности

Продолжительность занятия: 2/2 ч.

3. Указания по проведению лабораторного практикума

Цель и задачи выполнения лабораторных работ:

Цель: Изучить механизмы регуляторов и их право-применение при анализе объекта ИБ.

Методика *(определяется технологией изучения нормативно-правовых документов регулирующих область ИБ. и выполнения лабораторных работ (заданий) связанных с изучением требований руководящих документов в области ИБ.*

Этапы выполнения лабораторных работ *(Постановка задачи лабораторной работы. Ознакомление обучающегося с содержанием и объемом лабораторной работы. Порядок выполнения лабораторной работы. Регистрация результатов и оформление отчета о лабораторной работе. Заключительная часть лабораторной работы).*

Тематика лабораторных работ и задания к ним:

3.1. Требования к структуре

Структура лабораторной работы должна способствовать раскрытию темы: иметь титульный лист, содержание, введение, основную часть, заключение, список литературы.

3.2. Требования к содержанию (основной части)

1. Во введении обосновывается актуальность темы, определяется цель работы, задачи и методы исследования.

2. Основная часть работы раскрывает процесс проектирования заданного аппаратного устройства и должна содержать соответствующие таблицы или временные диаграммы, которые должны формироваться разрабатываемым устройством, принципиальную схему устройства и описание его работы.

3. В процессе изложения материала необходимо давать ссылки на используемую литературу.

4. Заключение должно содержать сделанные автором работы выводы, итоги исследования.

5. Вслед за заключением идет список литературы, который должен быть составлен в соответствии с установленными требованиями.

3.3. Требования к оформлению

Объём лабораторной работы – 5-6 страниц формата А 4, напечатанного с одной стороны текста (1,5 интервал, шрифт Times New Roman).

3.4.Тематика лабораторных работ

Лабораторная работа 1.

Тема: Введение в дисциплину, предмет и задачи программно-аппаратной защиты информации. Идентификация субъекта, понятие протокола идентификации, идентифицирующая информация. Основные подходы к защите данных от НСД. Шифрование, контроль доступа и разграничение доступа, иерархический доступ к файлу, защита сетевого файлового ресурса, фиксация доступа к файлам.

Цель занятия: выявить основные подходы к защите данных от НСД, принципы шифрования, контроля и разграничения доступа.

Продолжительность занятия – 4/3 ч.

Задание:

1. Изучить предмет и задачи программно-аппаратной защиты информации.
2. Идентификация субъекта, понятие протокола идентификации, идентифицирующая информация.
3. Основные подходы к защите данных от НСД.
4. Шифрование, контроль доступа и разграничение доступа, иерархический доступ к файлу, защита сетевого файлового ресурса, фиксация доступа к файлам.
5. Оформить отчет по проведенному исследованию.

Лабораторная работа 2.

Тема: Доступ к данным со стороны процесса, способы фиксации факта доступа, надежность систем ограничения доступа. Защита файлов от изменения. Электронная цифровая подпись (ЭЦП). Программно-аппаратные средства шифрования. Построение аппаратных компонент криптозащиты данных.

Цель занятия: выявить основные способы доступа к данным со стороны процесса, способы фиксации факта доступа, надежность систем ограничения доступа.

Продолжительность занятия – 4/3 ч.

Задание:

1. Доступ к данным со стороны процесса, способы фиксации факта доступа, надежность систем ограничения доступа.
2. Защита файлов от изменения. Электронная цифровая подпись (ЭЦП).
3. Программно-аппаратные средства шифрования.
4. Построение аппаратных компонент криптозащиты данных.

5. Оформить отчет по проведенному исследованию.

Лабораторная работа 3.

Тема: Защита алгоритма шифрования. Принцип чувствительной области и принцип главного ключа, необходимые и достаточные функции аппаратного средства криптозащиты. Пароли и ключи, организация хранения ключей. Методы и средства ограничения доступа к компонентам ЭВМ.

Цель занятия:

Продолжительность занятия – 4/3 ч.

Задание:

1. Защита алгоритма шифрования. Принцип чувствительной области и принцип главного ключа, необходимые и достаточные функции аппаратного средства криптозащиты.
2. Пароли и ключи, организация хранения ключей. Методы и средства ограничения доступа к компонентам ЭВМ.
3. Оформить отчет по проведенному исследованию.

Лабораторная работа 4.

Тема: Защита программ от несанкционированного копирования. Защита программ от изучения; защита от отладки, защита от дизассемблирования, защита от трассировки по прерываниям. Защита от разрушающих программных воздействий (РПВ). Компьютерные вирусы как особый класс РПВ. Необходимые и достаточные условия недопущения разрушающего воздействия. Понятие изолированной программной среды.

Цель занятия:

Продолжительность занятия – 4/3 ч.

Задание:

1. Защита программ от несанкционированного копирования. Защита программ от изучения; защита от отладки, защита от дизассемблирования, защита от трассировки по прерываниям.
2. Защита от разрушающих программных воздействий (РПВ). Компьютерные вирусы как особый класс РПВ.
3. Необходимые и достаточные условия недопущения разрушающего воздействия. Понятие изолированной программной среды.
4. Оформить отчет по проведенному исследованию.

4. Указания по проведению самостоятельной работы студентов

№ п/п	Наименование блока (раздела) дисциплины	Виды СРС
1.	**Тема 2. Международные стандарты информационной**	***Подготовка докладов по темам:*** 1. Предназначение стандартов информационной безопасности (ИБ), необходимость их использования. 2. Общие критерии безопасности информационных

	безопасности	технологий (стандарт ISO 15408). 3. Взаимосвязь между общими критериями и общей методологией оценки. 4. Структура технического отчета об оценке. 5. Стандарты для беспроводных сетей.
2.	**Тема 3. Отечественные стандарты информационной безопасности**	***Подготовка докладов по темам:*** 1. Стандарты в сети Internet. 2. Отечественные стандарты безопасности информационных технологий. 3. Нормативные документы по критериям оценки защищенности средств вычислительной техники (СВТ) и автоматизированных систем (АС). 4. Документы, регулирующие информационную безопасность. Достоинства ГОСТ Р ИСО/МЭК 15408 - 2002. 5. Структура функционального класса. 6. Структура функционального семейства.
3	**Тема 4. Критерии оценки доверенных компьютерных систем («Оранжевая книга»)**	***Подготовка докладов по темам:*** 1. Общая схема представления класса. 2. Структура функционального компонента. 3. Критерии оценки доверенных компьютерных систем («Оранжевая книга»). Назначение и структура требований. 4. Группы классов защищенности и их характеристики. 5. Руководящие документы Гостехкомиссии России (ФСТЭК). 6. Межсетевые экраны. Показатели защищенности. 7. Классификация АС и требования по защите информации. 8. Программное обеспечение средств защиты информации. 9. Общие критерии. Основные положения. 10. Структура и содержание профиля защиты. 11. Структура и содержание задания по безопасности.
4	**Тема 5. Руководящие документы Гостехкомиссии России (ФСТЭК).**	***Подготовка докладов по темам:*** 1. Функциональные требования безопасности. 2. Требования доверия. Методы оценки. Оценочные уровни доверия. 3. Основные положения концепции защиты СВТ и АС от НСД к информации 4. Средства вычислительной техники. Защита от НСД к информации. Показатели защищённости от НСД к информации 5. Автоматизированные системы. Защита от НСД к информации. Классификация. АС и требования по защите информации 6. ISO/IEC 17799:2005 7. ISO/IEC 27001:2005 8. BS 7799-3:2006

5.Указания по проведению контрольных работ для студентов факультета заочного обучения

6.1. Требования к структуре

Структура контрольной работы должна способствовать раскрытию темы: иметь титульный лист, содержание, введение, основную часть, заключение, список литературы.

5.2. Требования к содержанию (основной части)

1. Во введении обосновывается актуальность темы, определяется цель работы, задачи и методы исследования.
2. При определении целей и задач исследования необходимо правильно их формулировать. Так, в качестве цели не следует употреблять глагол «сделать». Правильно будет использовать глаголы «раскрыть», «определить», «установить», «показать», «выявить» и т.д.
3. Основная часть работы включает 2-4 вопроса, каждый из которых посвящается решению задач, сформированных во введении, и заканчивается констатацией итогов.
4. Приветствуется иллюстрация содержания работы таблицами, графическим материалом (рисунками, схемами и т.п.).
5. Необходимо давать ссылки на используемую литературу.
6. Заключение должно содержать сделанные автором работы выводы, итоги исследования.
7. Вслед за заключением идет список литературы, который должен быть составлен и оформлен с установленными требованиями. Если в работе имеются приложения, они оформляются на отдельных листах, и должны быть соответственно пронумерованы.

5.3. Требования к оформлению

Объём контрольной работы – 5-6 страниц формата А 4, напечатанного с одной стороны текста (1,5 интервал, шрифт Times New Roman).

5.4.Примерная тематика контрольных работ:

1. Сформулировать функциональные требования по безопасности к СВТ типового выделенного помещения органа муниципального управления.
2. Сформулировать функциональные требования по безопасности к СВТ типового выделенного помещения высшего учебного заведения.
3. Сформулировать функциональные требования по безопасности к СВТ и АС типовой туристической фирмы.
4. Сформулировать функциональные требования по безопасности к СВТ и АС выделенного помещения типового машиностроительного предприятия.
5. Сформулировать функциональные требования по безопасности к СВТ выделенного помещения типового торгового предприятия.
6. Построить профиль защиты для объекта оценки типового органа муниципального управления.

7. Построить профиль защиты для объекта оценки типового высшего учебного заведения.

8. Построить профиль защиты для объекта оценки типовой туристической фирмы.

9. Построить профиль защиты для объекта оценки типового машиностроительного предприятия.

10. Построить профиль защиты для объекта оценки типового торгового предприятия.

11. Разработать задание по безопасности и меры доверия для объекта оценки типового органа муниципального управления.

12. Разработать задание по безопасности и меры доверия для объекта оценки типового высшего учебного заведения.

13. Разработать задание по безопасности и меры доверия для объекта оценки типовой туристической фирмы.

14. Разработать задание по безопасности и меры доверия для объекта оценки типового торгового предприятия.

15. Разработать задание по безопасности и меры доверия для объекта оценки типового машиностроительного предприятия.

16. Разработать требования доверия для объекта оценки типового органа муниципального управления.

17. Разработать требования доверия для объекта оценки типового высшего учебного заведения.

18. Разработать требования доверия для объекта оценки типовой туристической фирмы.

19. Разработать требования доверия для объекта оценки типового торгового предприятия.

20. Разработать требования доверия для объекта оценки типового машиностроительного предприятия.

21. Произвести оценку по классам защищённости СВТ и АС типового органа муниципального управления.

22. Произвести оценку по классам защищённости СВТ и АС типового высшего учебного заведения.

23. Произвести оценку по классам защищённости СВТ и АС типовой туристической фирмы.

24. Произвести оценку по классам защищённости СВТ и АС типового торгового предприятия.

25. Произвести оценку по классам защищённости СВТ и АС типового машиностроительного предприятия.

26. Разработать модель управления рисками типового органа муниципального управления.

27. Разработать модель управления рисками типового высшего учебного заведения.

28. Разработать модель управления рисками типовой туристической фирмы.

29. Разработать модель управления рисками типового торгового предприятия.

30. Разработать модель управления рисками типового машиностроительного предприятия.

6. Перечень основной и дополнительной учебной литературы

Основная литература:

1.Ермакова, А. Ю. Методы и средства защиты компьютерной информации : учебное пособие / А. Ю. Ермакова. — Москва : РТУ МИРЭА, 2020. — 223 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/163844 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

2.Пугин, В. В. Защита информации в компьютерных информационных системах : учебное пособие / В. В. Пугин, Е. Ю. Голубничая, С. А. Лабада. — Самара : ПГУТИ, 2018. — 119 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/182299 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

3.Электронный документооборот и обеспечение безопасности стандартными средствами WINDOWS : учебное пособие / Л.М. Евдокимова, В.В. Корябкин, А.Н. Пылькин, О.Г. Швечкова. - Москва : КУРС, 2023. - 296 с. - ISBN 978-5-906923-24-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1902497 (дата обращения: 30.11.2022). – Режим доступа: по подписке.

4.Информационные технологии в документационном обеспечении управления и архивном деле : учебник для вузов / Н. Н. Кунаев, Т. В. Кондрашова, Е. В. Терентьева, А. Г. Фабричнов / под общ. ред. Н. Н. Куняева. - Москва : Логос, 2020. - 408 с. - ISBN 978-5-98704-786-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1211641 (дата обращения: 30.11.2022). – Режим доступа: по подписке.

5.Моргунов, А. В. Электронные системы документооборота : учебное пособие / А. В. Моргунов. - Новосибирск : Изд-во НГТУ, 2020. - 74 с. - ISBN 978-5-7782-4269-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/1870515 (дата обращения: 30.11.2022). – Режим доступа: по подписке.

Дополнительная литература:

6.Конфиденциальное делопроизводство и защищенный электронный документооборот : учебник / Н. Н. Куняев, А. С. Дёмушкин, Т. В. Кондрашова, А. Г. Фабричнов ; под общ. ред. Н. Н. Куняева. - 2-е изд., перераб. и доп. - Москва : Логос, 2020. - 500 с. - (Новая университетская библиотека). - ISBN 978-5-98704-711-8. - Текст : электронный. - URL: https://znanium.com/catalog/product/1212394 (дата обращения: 30.11.2022). – Режим доступа: по подписке.

7.Раздорожный, А. А. Документирование управленческой деятельности : учеб. пособие / А.А. Раздорожный. — Москва : ИНФРА-М, 2018. — 304 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-16-011744-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/969585 (дата обращения: 30.11.2022). – Режим доступа: по подписке.

8.Информационные технологии в документационном обеспечении управления и архивном деле : учебник для вузов / Н. Н. Кунаев, Т. В. Кондрашова, Е. В. Терентьева, А. Г. Фабричнов / под общ. ред. Н. Н. Куняева. - Москва : Логос,

2020. - 408 с. - ISBN 978-5-98704-786-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1211641 (дата обращения: 30.11.2022). – Режим доступа: по подписке.

7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

Интернет-ресурсы:

1. http://eup.ru/catalog/all-all.asp – научно-образовательный портал.
2. http://informika.ru/ – образовательный портал.
3. www.wikIsec.ru - Энциклопедия информационной безопасности. – Публикации, статьи.
4. **www.biblioclub.ru** - Универсальная библиотека онлайн.
5. **www.rucont.ru** - ЭБС «Руконт».
6. http://www.academy.it.ru/ - академия АЙТИ.
7. http://www.minfin.ru - Официальный сайт Министерства финансов Российской Федерации
8. http://www.gov.ru/ - Официальный сервер органов государственной власти Российской Федерации.
9. http://www.fsb.ru/ - Официальный сайт Федеральной Службы Безопасности
10. http://www.fstec.ru/ - Официальный сайт Федеральной Службы по Техническому Экспортному контролю

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю)

Перечень программного обеспечения: MSOffice, PowerPoint.

Информационные справочные системы:

1.Электронные ресурсы образовательной среды Университета.

2.Информационно-справочные системы (Консультант+; Гарант).

3.Рабочая программа и методическое обеспечение по курсу «Нормативные акты м стандарты по информационной безопасности»