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
«___»_____2023г.

ИНСТИТУТ
ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ»

Направление подготовки: 09.03.02 Информационные системы и технологии

Направленность (профиль): высокопроизводительные вычислительные и телекоммуникационные интеллектуальные системы и комплексы

Уровень высшего образования: бакалавриат

Форма обучения: очная, 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: Баранова О.М. **Рабочая программа дисциплины «Безопасность информационных систем». – Королев МО: Технологический университет, 2023 г.**

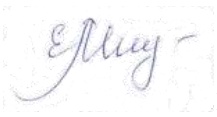
Рецензент: к.т.н., доц. Сазонов С.Ю.

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки бакалавров 09.03.02 Информационные системы и технологии, учебного плана, утвержденного Ученым советом Технологического университета, протокол № 9 от 11.04.2023 года.

Рабочая программа рассмотрена и одобрена на заседании кафедры:

Заведующий кафедрой (ФИО, ученая степень, звание, подпись)	Сазонов С.Ю., к.т.н., доц. 			
Год утверждения (переутверждения)	2023	2024	2025	2026
Номер и дата протокола заседания кафедры	№ 8 от 29.03.2023			

Рабочая программа согласована:

Руководитель ОПОП  к.т.н., доц. Е.Г. Макарова.

Рабочая программа рекомендована на заседании УМС:

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

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

Целью изучения дисциплины является:

1. Формирование базовых знаний и практических навыков обеспечения безопасности информационных систем.
2. Развитие творческого и исследовательского подхода к изучению технических дисциплин студенчества.
3. Подготовка студентов к видам профессиональной деятельности: проектной, производственно-технологической, организационно-управленческой, аналитической и научно-исследовательской.
4. Приобретение студентами знаний и представлений об основных принципах и закономерностях функционирования современной вычислительной техники и их информационной безопасности.
5. Приобретение студентами теоретических сведений и практических навыков, позволяющих формировать устройства вычислительной техники в защищенном исполнении с заданными техническими характеристиками.

В процессе обучения студент приобретает и совершенствует следующие компетенции:

Общие профессиональные компетенции:

ОПК-4 Способен участвовать в разработке технической документации, связанной с профессиональной деятельностью с использованием стандартов, норм и правил;

Профессиональные компетенции:

– ПК-7 способен выполнять работы по обслуживанию программно-аппаратными средствами сетей и инфокоммуникаций.

Основными **задачами** дисциплины являются:

- формирование целостного компендиума знаний правовых и методических документов в области обеспечения безопасности информационных систем (ИС);
- изучение базовых моделей угроз информационной безопасности и возможных моделей нарушителей для обеспечения проектирования ИС;
- изучение национальных стандартов и методических положений по оценке информационной защищённости при анализе и проектировании защищённых ИС;
- подготовка студентов к деятельности, связанной с созданием, эксплуатацией и обслуживанием (сопровождением) защищённых ИС;
- привитие навыков работы с проектной и технической документацией по проектированию защищённых ИС и оценке их эффективности;
- формирование знаний по проведению аудита информационной безопасности в организации;
- формирование представлений о принципах обеспечения информационной безопасности при использовании вычислительной техники.

Показатель освоения компетенции отражают следующие индикаторы:

Трудовые действия:

- Имеет навыки составления технической документации на различных этапах жизненного цикла информационной системы.
- Разрабатывает техническое задание на информационную систему

Необходимые умения:

- Умеет применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы.
- Умеет разрабатывать концепцию информационной системы

Необходимые знания:

- Знает основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы.
- Знает цели создания информационной системы

2. Место дисциплины (модуля) в структуре ОПОП ВО

Дисциплина «**Безопасность информационных систем»**» относится к обязательной части основной профессиональной образовательной программы подготовки бакалавров по направлению подготовки 09.03.02 «Информационные системы и технологии».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах модуля: «Математика», «Информатика» и компетенциях ОПК-1, ОПК-2, ОПК-5, ОПК-6, ОПК-7, ОПК-8, ПК-2, ПК-3, ПК-4, ПК-6, ПК-11, ПК-14.

3.Объем дисциплины (модуля) и виды учебной работы

Общая трудоемкость дисциплины для студентов очной формы составляет 9 зачетных единиц, 324 часа.

Таблица1

Виды занятий	Всего часов	Семестр 5	Семестр 6	Семестр	Семестр
Общая трудоемкость	**324**	**112**	**112**		
ОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	**112**	**48**	**64**		
Лекции (Л)	**32**	**16**	**16**		
Практические занятия (ПЗ)	**80**	**32**	**48**		
Практическая подготовка	**32**	**16**	**16**		
Самостоятельная работа	**212**	**96**	**116**		
Курсовые работы (проекты)	+	-	+		
Расчетно-графические работы	-	-	-		
Контрольная работа, домашнее задание	+ -	+ -	+ -		

Текущий контроль знаний (7 - 8, 15 - 16 недели)	**тест**	**тест**	**тест**		
Вид итогового контроля	**Экзамен, Зачёт с оценкой**	**Зачёт с оценкой**	**Экзамен**		
ЗАОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	**32**	**32**			
Лекции (Л)	**8**	**8**			
Практические занятия (ПЗ)	**24**	**24**			
Практическая подготовка	**24**	**24**			
Самостоятельная работа	**292**	**292**			
Курсовые, расчетно-графические работы	**+**	**+**			
Контрольная работа, домашнее задание	**+**	**+**			
Вид итогового контроля	**Зачет с оценкой, Экзамен**	**Зачет с оценкой ,Экзамен**			

4. Содержание дисциплины

4.1.Темы дисциплины и виды занятий

Таблица 2

Наименование тем	Лекции, час. Оч/заоч	Практические занятия, Час Оч/заоч	Занятия в интерактивной форме, час Оч/заоч	Практическая подготовка, оч/заоч	Код компетенций
Тема 1. Основы защиты информации. Информационная безопасность	**6/1**	**12/2**	**6/4**	**6/4**	**ОПК-4 , ПК-7**
Тема 2. Методы несанкционированного доступа к информационным системам	**10/1**	**20/6**	**10/6**	**10/6**	
Тема 3. Системный подход к обеспечению безопасности информационных систем	**22/3**	**20/8**	**8/8**	**8/8**	

Наименование тем	Лекции, час. Оч/заоч	Практические занятия, Час Оч/заоч	Занятия в интерактивной форме, час Оч/заоч	Практическая подготовка, оч/заоч	Код компетенций
Тема 4. Комплексная система защиты информации (КСЗИ)	**6/2**	**20/4**	**4/4**	**4/4**	
Тема 5. Проектирование комплексной системы защиты информации (КСЗИ) в ИС	**4/1**	**8/4**	**4/2**	**4/2**	
Итого:	**48/8**	**80/24**	**32/24**	**32/24**	

4.2. Содержание тем дисциплины

Тема 1. Основы защиты информации. Информационная безопасность

Понятия защиты информации и информационной безопасности. Основные составляющие информационной безопасности. Свойства информации, важные с точки зрения обеспечения информационной безопасности. Виды и анализ угроз информационных систем, источники угроз.

Тема 2. Методы несанкционированного доступа к информационным системам

Методы нарушения конфиденциальности, целостности и доступности информации. Причины, виды, каналы утечки и искажения информации. Анализ возможных методов несанкционированного доступа.

Тема 3. Системный подход к обеспечению безопасности информационных систем

Законодательный уровень системы обеспечения информационной безопасности: законодательные акты, нормативные документы. Административный уровень системы обеспечения информационной безопасности: политика безопасности, анализ и оценка информационных рисков. Процедурный (организационный) уровень системы обеспечения информационной безопасности. Программно-технический уровень системы обеспечения информационной безопасности: сервисы безопасности.

Тема 4. Комплексная система защиты информации (КСЗИ)

Структура КСЗИ от НСД в ИС. Подсистемы КСЗИ. Подсистема контроля доступа. Подсистема охранно-пожарной сигнализации.

Подсистема автоматического пожаротушения. Подсистема контроля параметров окружающей среды. Подсистема обеспечения бесперебойного энергоснабжения. Подсистема видеонаблюдения. Подсистема ИБ. Подсистема антивирусной защиты. Подсистема парольной защиты. Подсистема защиты электронных документов. Подсистема ИБ локальной вычислительной сети (ЛВС). Подсистема защиты систем и каналов связи. Подсистема ИБ технологий обработки информации. Подсистема ИБ фонда алгоритмов и программ (ФАП). Центр управления ключевыми системами. Подсистема аудита ИБ.

Тема 5. Проектирование комплексной системы защиты информации (КСЗИ) в ИС

Этапы проектирования комплексной системы информационной безопасности ИС и требования к ним: предпроектное обследование, техническое задание, техническое проектирование, рабочее проектирование, испытания и внедрение в эксплуатацию, сопровождение при создании защищенных ИС.

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

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

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

Структура фонда оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине приведена в Приложении 1.

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

Основная литература:

1. Бирюков А. Информационная безопасность / А. Бирюков . - Москва : ДМК Пресс, 2017. - с. URL: https://e.lanbook.com/book/93278
2. Рябко Б.Я., Фионов А.Н. Основы современной криптографии и стеганографии – 2-е издание- М.: Горячая линия – Телеком, 2013. – 232с.

Дополнительная литература:

1. Гришина Н.В.Информационная безопасность предприятия : учебное пособие / Н.В. Гришина. - 2-е изд., доп. - М. ; М. : ФОРУМ : НИЦ ИНФРА-М, 2015. - 240 с. - (Высшее образование - бакалавриат)
2. Кияев, В. Безопасность информационных систем / В. Кияев; О. Граничин. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 192 с. URL: http://biblioclub.ru/index.php?page=book&id=429032

8. Перечень ресурсов информационно-телекоммуникационной сети интернет, необходимых для освоения дисциплины (модуля)

1. ISO27000.ru (портал по ИБ, аналитика, информация по законодательству и стандартам, блоги, каталоги ресурсов и ПО).
2. WinSecurity.ru (статьи, документация, новости по безопасности Windows).
3. Журнал Информационная безопасность (публикации, статьи, обзоры, форум).
4. http://www.gov.ru - сервер органов государственной власти Российской Федерации.
5. www.wikIsec.ru - Энциклопедия информационной безопасности. – Публикации, статьи.
6. www.biblioclub.ru - Универсальная библиотека онлайн.
7. www.rucont.ru - ЭБС «Руконт».
8. http://www.minfin.ru - Официальный сайт Министерства финансов Российской Федерации
9. http://www.gov.ru/ - Официальный сервер органов государственной власти Российской Федерации.
10. http://www.fsb.ru/ - Официальный сайт Федеральной Службы Безопасности
11. http://www.fstec.ru/ - Официальный сайт Федеральной Службы по Техническому Экспортному контролю

9. Методические указания для обучающихся по освоению дисциплины (модуля)

Методические указания для обучающихся, по освоению дисциплины, приведены в Приложении 2.

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

Перечень программного обеспечения: Microsoft Office или свободно распространяемые аналоги, ПО комплекса «Основы компьютерно-информационной безопасности»

Информационные справочные системы:

1. Ресурсы информационно-образовательной среды Технологического университета.
2. Рабочая программа и методическое обеспечение по дисциплине: «Безопасность информационных систем»

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

Лекционные занятия:

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

Практические занятия:

- компьютерный класс с проектором для интерактивного обучения и проведения занятий в форме слайд-презентаций, оборудованный современными лицензионными программно-техническими средствами: операционная система не ниже WindowsXP, эмуляции виртуальных машин (VM-vare, VM-box или др.)
- 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

ИНСТИТУТ
ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ
(Приложение 1 к рабочей программе)

Направление подготовки: 09.03.02 Информационные системы и технологии

Направленность (профиль): высокопроизводительные вычислительные и телекоммуникационные интеллектуальные системы и комплексы

Уровень высшего образования: бакалавриат

Форма обучения: очная, заочная

Королев 2023

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

№ п/п	Индекс компе-тенции	Содержание компетенции (или ее части)*	Раздел дисциплины, обеспечивающий формирование компетенции (или ее части)	В результате изучения раздела дисциплины, обеспечивающего формирование компетенции (или ее части), обучающийся приобретает:		
				Трудовые действия	Необходимые умения	Необходимые знания
1	ОПК-4	Способен участвовать в разработке технической документации, связанной с профессиональной деятельностью с использованием стандартов, норм и правил	Тема 1-8	Владеть методами поиска, сбора и обработки, критического анализа и синтеза информации; методикой системного подхода для решения поставленных задач	Уметь применять методики поиска, сбора и обработки информации; осуществлять критический анализ и синтез информации, полученной из разных источников; применять системный подход для решения поставленных задач	Знать методики поиска, сбора и обработки информации; актуальные российские и зарубежные источники информации в сфере профессиональной деятельности; метод системного анализа. .
2	ПК-7	способен выполнять работы по обслуживанию программно-аппаратными средствами сетей и инфокоммуникаций.	Тема 1-8	Разрабатывает техническое задание на информационную систему	Умеет разрабатывать концепцию информационной системы	Знает цели создания информационной системы

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

Код компетенции	Инструменты, оценивающие сформированность компетенции	Показатель оценивания компетенции	Критерии оценки
ОПК-4 ПК-7	Практическое задание	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 освоена) – 2 и менее баллов	Проводится в форме письменной работы Время, отведенное на процедуру – 60 мин. Неявка – 0. Критерии оценки: 1.Соответствие ответа заявленной тематике (0-5 баллов). Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся в срок не позднее 1 недели после проведения процедуры – для текущего контроля. Оценка проставляется в электронный журнал.
ОПК-4 ПК-7	Контрольная работа	**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 освоена) – 2 и менее баллов	Проводится в форме письменной контрольной работы (электронный документ). Время, отведенное на процедуру – 40 - 60 мин. Неявка – 0. Критерии оценки: 1.Соответствие ответа заявленной тематике (0-5 баллов). Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся в срок не позднее 1 недели после проведения процедуры – для текущего контроля. Оценка проставляется в электронный журнал.

3. Типовые контрольные, практические 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 практических заданий:

1. Проанализировать возможные методы несанкционированного доступа в отношении информационной системы конкретной организации.
2. Определить угрозы информационной безопасности в отношении информационной системы конкретной организации и меры противодействия им.
3. Проанализировать технические каналы несанкционированного доступа к информации и технические средства несанкционированного доступа.
4. Проанализировать технические средства зашиты от несанкционированного доступа к информации.
5. Проанализировать хакерские методы получения несанкционированного доступа к информации и методы защиты.
6. Проанализировать методы получения несанкционированного доступа к информации, основанные на применении социальной инженерии и методы защиты.
7. На основе Уголовного кодекса РФ и Кодекса об административных правонарушениях РФ проанализировать ситуации кейсов, определить состав правонарушения в части нарушения информационной безопасности.
8. На основе Федерального закона от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации» (до ст. 9 включительно) проанализировать ситуации кейсов, определить состав правонарушения в части нарушения информационной безопасности.
9. На основе Федерального закона от 27.07.2006 №152-ФЗ "О персональных данных проанализировать ситуации кейсов, определить состав правонарушения в части нарушения информационной безопасности.
10. Произвести сравнительный анализ требований 152-ФЗ "О персональных данных" и "Общего регламента по защите данных" ЕС (GDPR).
11. Разработать Политику безопасности организации в соответствии с вариантом задания.
12. Выполнить оценку информационных рисков в отношении информационной системы конкретной организации одним из предлагаемых методов.
13. Разработать перечень и описание мер процедурного (организационного) уровня информационной безопасности в соответствии с ранее выявленными угрозами и информационными рисками для конкретной организации.

Примерная тематика заданий на контрольную работу:

1. В соответствии с номером варианта задания на основе архитектурного плана здания проанализировать достоинства и недостатки помещений указанного этажа с точки зрения размещения переговорной комнаты, выбрать определенное помещение для размещения переговорной комнаты, предложить организационные и технические решения для обеспечения безопасности проектируемой переговорной комнаты.

2. В соответствии с номером варианта задания на основе законодательных актов информационного права проанализировать ситуации кейсов, определить состав правонарушения в части нарушения информационной безопасности.

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

Формой контроля знаний по дисциплине «Безопасность информационных систем» являются две текущие аттестации в виде тестов в течение каждого семестра и промежуточная аттестация в виде зачета с оценкой (5 семестр) и экзамена (6 семестр).

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
Согласно графика учебного процесса	тестирование	ОПК-4 ПК-7	20 вопросов	Компьютерное тестирование; время, отведенное на процедуру - 30 минут	Результаты тестирования предоставляются в день проведения процедуры	Критерии оценки определяются процентным соотношением. Не явка - Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%.

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
Согласно графика учебного процесса	тестирование	ОПК-4 ПК-7	20 вопросов	Компьютерное тестирование; время, отведенное на процедуру – 30 минут	Результаты тестирования предоставляются в день проведения процедуры	Критерии оценки определяются процентным соотношением. Не явка -0 Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%. Максимальная оценка – 5 баллов.
Согласно графика учебного процесса	Зачет с оценкой	ОПК-4 ПК-7	1 вопрос	Зачет с оценкой проводится в устной форме, путем ответа на вопросы. Время, отведенное на процедуру – 30 минут.	Результаты предоставляются в день проведения зачета с оценкой	Критерии 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

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
						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; «**Неудовлетворительно**»: • 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.
Согласно графика учебного процесса	Защита курсовой работы	ОПК-4 ПК-7	3 вопроса	Защита курсовой работы проводится в устной форме, путем ответа на вопросы.	Результаты предоставляются в день проведения экзамена	Критерии оценки: «**Отлично**»: • знание основных понятий предмета; • умение использовать и применять полученные знания на практике;

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
				Время, отведенное на процедуру – 20 минут.		• работа на практических занятиях; • знание основных научных теорий, изучаемых предметов; • курсовая работа, выполненная и оформленная в соответствии с требованиями; • решения, предлагаемые в курсовой работе, соответствуют целям и задачам выполнения курсовой работы; • ответ на вопросы по тематике курсовой работы. «**Хорошо**»: • знание основных понятий предмета; • умение использовать и применять полученные знания на практике; • работа на практических занятиях; • курсовая работа, выполненная и оформленная в соответствии с требованиями; • решения, предлагаемые в курсовой работе, не полностью соответствуют целям и задачам

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
						выполнения курсовой работы; • не полный ответ на вопросы по тематике курсовой работы. «У**довлетвори-тельно**»: • демонстрирует частичные знания по темам дисциплин; • незнание неумение использовать и применять полученные знания на практике; • не работал на практических занятиях; • курсовая работа, выполненная и оформленная в соответствии с требованиями; • решения, предлагаемые в курсовой работе, частично соответствуют целям и задачам выполнения курсовой работы; • частичный ответ на вопросы по тематике курсовой работы. «**Неудовлетворительно**»: • демонстрирует частичные знания по темам дисциплин; • незнание основных понятий предмета; • неумение ис-

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
						пользовать и применять полученные знания на практике; • не работал на практических занятиях; • курсовая работа, выполненная и оформленная в соответствии с требованиями; • решения, предлагаемые в курсовой работе, не соответствуют целям и задачам выполнения курсовой работы; • не отвечает на вопросы по тематике курсовой работы.
В соответствии с КУГ	Экзамен	ОПК-4 ПК-7	2 вопроса	Экзамен проводится в устной форме, путем ответа на вопросы. Время, отведенное на процедуру – 30 минут.	Результаты предоставляются в день проведения экзамена	Критерии 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

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
						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; «**Неудовлетворительно**»: • 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.

4.1. Типовые вопросы, выносимые на тестирование

1. Система информационного законодательства включает в себя
   - только правовые акты федеральных органов
   - правовые акты федеральных органов и акты органов субъектов РФ
   - акты органов субъектов РФ и нормативно-справочную документацию
   - правовые акты федеральных органов и нормативно-справочную документацию

2. Гражданин (физическое лицо) имеет право на получение от государственных органов, органов местного самоуправления, их должностных лиц в порядке, установленном законодательством Российской Федерации,
   - информации, непосредственно затрагивающей его права и свободы
   - информации, связанной с реализацией его прав собственности
   - любой интересующей его информации
   - информации, связанной с функционированием государственных органов

3. Организация имеет право на получение от государственных органов, органов местного самоуправления
   - информации, связанной с профессиональной тайной
   - информации, непосредственно касающейся прав и обязанностей этой организации
   - любой интересующей ее информации
   - информации, определяющей физических лиц

4. Зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель – это
   - защищаемая информация
   - документированная информация
   - объект защиты информации
   - электронный документ

5. Документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах – это

- защищаемая информация
- объект защиты информации
- документированная информация
- электронный документ

6. Лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам – это

- собственник информации
- пользователь информации
- обладатель информации
- автор информации

7. Назовите принципы, на которых основывается правовое регулирование отношений, возникающих в сфере информации, информационных технологий и защиты информации (возможно несколько правильных вариантов ответа):

- неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия
- разнообразие информации и свобода ее предоставления, если иное не определено обладателем информации
- установление ограничений доступа к информации только ее авторами
- открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами
- обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации

8. В зависимости от категории доступа к ней информация подразделяется на

- публичную информацию и информацию, доступ к которой оп-

ределяется ее степенью секретности
- информацию, свободно распространяемую, и информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях
- информацию, свободно распространяемую и информацию, доступ к которой определяется ее степенью секретности
- общедоступную информацию и на информацию, доступ к которой ограничен федеральными законами

9. Назовите информацию, к которой не может быть ограничен доступ в соответствии с Федеральным законом от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации» (возможно несколько правильных вариантов ответа):
- информации, защищенной авторским правом
- нормативным правовым актам, затрагивающим права, свободы и обязанности человека и гражданина, а также устанавливающим правовое положение организаций и полномочия государственных органов, органов местного самоуправления;
- информации о состоянии окружающей среды
- информации о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных и внебюджетных средств
- информации, не относящейся к государственной тайне
- иной информации, недопустимость ограничения доступа к которой установлена федеральными законами

10. Режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду, – это
- государственная тайна
- служебная тайна
- коммерческая тайна
- профессиональная тайна

11. Информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности, подлежащая защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации, – это

– государственная тайна
– служебная тайна
– коммерческая тайна
– профессиональная тайна

12. Срок исполнения обязанностей по соблюдению конфиденциальности информации, составляющей профессиональную тайну,
– может быть ограничен только с согласия гражданина (физического лица)
– определяется в зависимости от степени секретности информацию
– не может быть ограничен
– может быть ограничен только по решению суда

13. Совокупность правил, процедур, практических методов и руководящих принципов в области информационной безопасности, используемых организацией в своей деятельности, – это
– методика информационной безопасности
– политика информационной безопасности
– руководящий документ по информационной безопасности
– законодательный акт в сфере информационной безопасности

14. Меры верхнего уровня политики информационной безопасности предусматривают (возможно несколько правильных вариантов ответа):
– общее описание запрещенных действий и наказаний за них
– условия доступа к данным для чтения и модификации
– условия доступа к удаленным сервисам
– формулировку целей, которые преследует организация в области информационной безопасности
– определение ресурсов, требующихся для обеспечения информационной безопасности

15. Меры среднего уровня политики информационной безопасности предусматривают (возможно несколько правильных вариантов ответа):
– применение различных технологических решений
– условия доступа к данным для чтения и модификации
– условия доступа к удаленным сервисам
– правила взаимодействия с внешней информационной средой
– формулировку целей, которые преследует организация в области информационной безопасности

16. Меры нижнего уровня политики информационной безопасности предусматривают (возможно несколько правильных вариантов ответа):

- общее описание запрещенных действий и наказаний за них
- условия доступа к данным для чтения и модификации
- формулировку управленческих решений по вопросам реализации программы безопасности
- формулировку целей, которые преследует организация в области информационной безопасности
- определение прав доступа к объектам
- организация удаленного доступа к ресурсам

17. Формирование программы работ в области информационной безопасности и обеспечение ее выполнения путем выделения необходимых ресурсов происходит в рамках

- законодательного уровня информационной безопасности
- процедурного (организационного) уровня информационной безопасности
- программно-технического уровня информационной безопасности
- административного уровня информационной безопасности

18. Решение задач обеспечения информационной безопасности, связанных с участием персонала организации, происходит на:

- законодательном уровне информационной безопасности
- процедурном (организационном) уровне информационной безопасности
- программно-техническом уровне информационной безопасности
- административном уровне информационной безопасности

19. Назовите задачи, решаемые на процедурном (организационном) уровне информационной безопасности (возможно несколько правильных вариантов ответа)

- управления доступом
- обеспечения физической защиты
- идентификации и аутентификации
- поддержание работоспособности
- планирование восстановительных работ
- контроля целостности

20. Назовите принципы, применяющиеся на процедурном (организационном) уровне информационной безопасности для решения задач управления персоналом (возможно несколько правильных вариантов ответа)

- принцип разделения обязанностей
- принцип определения мотивации
- принцип равномерного распределения задач
- принцип минимизации привилегий
- принцип закрепления обязанностей

21. Распределение ролей и ответственности таким образом, что бы один человек не мог нарушить критически важный для организации процесс - это

- принцип разделения обязанностей
- принцип равномерного распределения задач
- принцип минимизации привилегий
- принцип закрепления обязанностей

22. Выделение пользователям только тех прав доступа, которые необходимы им для выполнения служебных обязанностей - это

- принцип разделения обязанностей
- принцип равномерного распределения задач
- принцип минимизации привилегий
- принцип закрепления обязанностей

23. К мерам физической защиты на процедурном (организационном) уровне информационной безопасности относятся (возможно несколько правильных вариантов ответа):

- защита поддерживающей инфраструктуры
- управление носителями
- анализ защищенности
- защита от перехвата данных
- физическое управление доступом
- обеспечение отказоустойчивости

4.3. Типовые вопросы, выносимые на зачет с оценкой (5 семестр)

1. Понятие национальной безопасности. Виды безопасности. Понятие информационной безопасности.
2. Основные составляющие информационной безопасности
3. Понятие защиты информации. Виды защиты информации
4. Свойства информации, значимые с точки зрения ее защиты
5. Угрозы информационной безопасности. Основные понятия

6. Классификация угроз информационной безопасности
7. Методы нарушения конфиденциальности информации
8. Методы нарушения целостности информации
9. Методы нарушения доступности информации
10. Причины, виды утечки и искажения информации
11. Каналы утечки и искажения информации
12. Анализ возможных методов несанкционированного доступа - Терминалы информационной системы. Физические терминалы
13. Анализ возможных методов несанкционированного доступа - Терминалы информационной системы. Удаленные терминалы
14. Анализ возможных методов несанкционированного доступа - Получение доступа на основе ошибок администратора и пользователей
15. Анализ возможных методов несанкционированного доступа - Получение доступа на основе ошибок в реализации
16. Анализ возможных методов несанкционированного доступа - Хакерские атаки
17. Анализ возможных методов несанкционированного доступа – Доступ к материальным объектам
18. Анализ возможных методов несанкционированного доступа - Технические каналы утечки информации
19. Анализ угроз информационной безопасности и методов несанкционированного доступа при проектировании переговорной комнаты
20. Анализ возможных методов несанкционированного доступа - Социальная психология и иные способы получения доступа

4.4. Типовые вопросы, выносимые на экзамен (6 семестр)

1. Законодательный уровень информационной безопасности. Основные законодательные акты в области информационной безопасности.
2. Законодательный уровень информационной безопасности. Законодательные акты в области информационной безопасности. Федеральный закон "Об информации, информационных технологиях и о защите информации". Основные понятия
3. Законодательный уровень информационной безопасности. Законодательные акты в области информационной безопасности. Федеральный закон "Об информации, информационных технологиях и о защите информации". Право на доступ к информации, ограничения на доступ к информации
4. Законодательный уровень информационной безопасности. Законодательные акты в области информационной безопасности. Федеральный закон "Об информации, информационных технологиях и о защите информации". Обязанности организатора распространения информации в сети «Интернет»
5. Законодательный уровень информационной безопасности. Законодательные акты в области информационной безопасности. Федеральный закон "Об информации, информационных технологиях и о защите ин-

формации". Особенности распространения информации в социальных сетях

6. Законодательный уровень информационной безопасности. Законодательные акты в области информационной безопасности. Федеральный закон "Об информации, информационных технологиях и о защите информации". Организация защиты информации
7. Законодательный уровень информационной безопасности. Законодательные акты в области информационной безопасности. Федеральный закон «Об электронной подписи». Основные понятия
8. Законодательный уровень информационной безопасности. Законодательные акты в области информационной безопасности. Федеральный закон «О персональных данных». Принципы и условия обработки персональных данных
9. Законодательный уровень информационной безопасности. Законодательные акты в области информационной безопасности. Федеральный закон «О персональных данных». Особенности обработки персональных данных, разрешенных субъектом персональных данных для распространения
10. Законодательный уровень информационной безопасности. Законодательные акты в области информационной безопасности. Федеральный закон "О деятельности иностранных лиц в информационно-телекоммуникационной сети "Интернет" на территории Российской Федерации"
11. Законодательный уровень информационной безопасности. Стандарты и спецификации в области информационной безопасности - "Критерии оценки доверенных компьютерных систем"
12. Законодательный уровень информационной безопасности. Стандарты и спецификации в области информационной безопасности – Семейство международных стандартов ISO/IEC 27000 Информационные технологии - Методы защиты
13. Законодательный уровень информационной безопасности. Стандарты и спецификации в области информационной безопасности – Общий регламент по защите данных (General Data Protection Regulation, GDPR)
14. Законодательный уровень информационной безопасности. Стандарты и спецификации в области информационной безопасности – стандарты РФ в области информационной безопасности
15. Административный уровень информационной безопасности. Политика безопасности.
16. Административный уровень информационной безопасности. Управление информационными рисками
17. Процедурный (организационный) уровень информационной безопасности. Управление персоналом
18. Процедурный (организационный) уровень информационной безопасности. Физическая защита
19. Процедурный (организационный) уровень информационной безопасности. Поддержание работоспособности

20. Процедурный (организационный) уровень информационной безопасности. Реагирование на нарушения режима безопасности
21. Процедурный (организационный) уровень информационной безопасности. Планирование восстановительных работ
22. Программно-технический уровень информационной безопасности. Сервисы безопасности
23. Идентификация и аутентификация - Парольная идентификация/аутентификация
24. Идентификация и аутентификация - Идентификация/аутентификация с помощью физических объектов
25. Идентификация и аутентификация - Идентификация/аутентификация с помощью графических объектов
26. Идентификация и аутентификация - Идентификация/аутентификация с помощью биометрических данных
27. Идентификация и аутентификация - Идентификация/аутентификация по местонахождению
28. Управление доступом. Мандатное управление доступом
29. Управление доступом. Избирательное управление доступом
30. Управление доступом. Ролевое управление доступом
31. Протоколирование и аудит
32. Криптографические методы защиты. Классификация алгоритмов шифрования
33. Криптографические методы защиты. Особенности симметричных блочных алгоритмов шифрования
34. Криптографические методы защиты. Особенности симметричных потоковых алгоритмов шифрования
35. Криптографические методы защиты. Особенности симметричных смешанных алгоритмов шифрования
36. Криптографические методы защиты. Особенности асимметричных алгоритмов шифрования
37. Контроль целостности
38. Обеспечение отказоустойчивости
39. Экранирование
40. Анализ защищенности
41. Туннелирование. VPN
42. Интегральная информационная безопасность
43. Современные программно-технические средства защиты информации
44. Структура КСЗИ от НСД в ИС.
45. Подсистемы КСЗИ.
46. Подсистема контроля доступа.
47. Подсистема охранно-пожарной сигнализации.
48. Подсистема автоматического пожаротушения.
49. Подсистема контроля параметров окружающей среды.
50. Подсистема обеспечения бесперебойного энергоснабжения.
51. Подсистема видеонаблюдения.
52. Подсистема ИБ.

53. Подсистема антивирусной защиты.
54. Подсистема парольной защиты.
55. Подсистема защиты электронных документов.
56. Подсистема ИБ локальной вычислительной сети (ЛВС).
57. Подсистема защиты систем и каналов связи.
58. Подсистема ИБ технологий обработки информации.
59. Подсистема ИБ фонда алгоритмов и программ (ФАП).
60. Этапы проектирования комплексной системы информационной безопасности ИС и требования к ним

ИНСТИТУТ
ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ БЕЗОПАНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ

(Приложение 2 к рабочей программе)

Направление подготовки: 09.03.02 Информационные системы и технологии
Направленность (профиль): высокопроизводительные вычислительные и телекоммуникационные интеллектуальные системы и комплексы

Уровень высшего образования: бакалавриат
Форма обучения: очная, заочная

Королев
2023

1. Общие положения

Цель дисциплины:

- формирование базовых знаний и практических навыков обеспечения безопасности информационных систем;
- развитие творческого и исследовательского подхода к изучению технических дисциплин студенчества;
- подготовка студентов к видам профессиональной деятельности: проектной, производственно-технологической, организационно-управленческой, аналитической и научно-исследовательской;
- приобретение студентами знаний и представлений об основных принципах и закономерностях функционирования современной вычислительной техники;
- приобретение студентами теоретических сведений и практических навыков, позволяющих формировать устройства вычислительной техники с заданными техническими характеристиками.

Задачи дисциплины:

- формирование целостного компендиума знаний правовых и методических документов в области обеспечения безопасности информационных систем (ИС);
- изучение базовых моделей угроз информационной безопасности и возможных моделей нарушителей для обеспечения проектирования ИС;
- изучение национальных стандартов и методических положений по оценке информационной защищённости при анализе и проектировании защищённых ИС;
- подготовка студентов к деятельности, связанной с созданием, эксплуатацией и обслуживанием (сопровождением) защищённых ИС;
- привитие навыков работы с проектной и технической документацией по проектированию защищённых ИС и оценке их эффективности.
- формирование знаний по проведению аудита информационной безопасности в организации;
- изучение и привитие навыков применения национальных стандартов, нормативных и методических документов в области управления информационной безопасностью;
- формирование представлений о принципах обеспечения информационной безопасности при использовании вычислительной техники;
- изучение принципов построения и работы основных цифровых узлов;
- приобретение опыта выбора элементной базы и типовых цифровых узлов вычислительной техники.

2. Указания по проведению практических занятий

Практическое занятие 1-6
Вид практического занятия**:** смешанная форма практического занятия.
Образовательная технология: кейс-технология
Тема и содержание практического занятия: Основы защиты информации. Информационная безопасность
Продолжительность занятия – 12 /2ч.

Практическое занятие 7-16
Вид практического занятия**:** смешанная форма практического занятия.
Образовательная технология: кейс-технология
Тема и содержание практического занятия: Методы несанкционированного доступа к информационным системам
Продолжительность занятия – 20/6 ч.

Практическое занятие 17-26
Вид практического занятия**:** смешанная форма практического занятия.
Образовательная технология: кейс-технология
Тема и содержание практического занятия: Системный подход к обеспечению безопасности информационных систем
Продолжительность занятия – 20/8 ч.

Практическое занятие 27-36
Вид практического занятия**:** смешанная форма практического занятия.
Образовательная технология: кейс-технология
Тема и содержание практического занятия: Комплексная система защиты информации (КСЗИ)
Продолжительность занятия – 20/4 ч.

Практическое занятие 37-40
Вид практического занятия**:** смешанная форма практического занятия.
Образовательная технология: командная работа
Тема и содержание практического занятия: Проектирование комплексной системы защиты информации (КСЗИ) в ИС
Продолжительность занятия – 8/4 ч.

3. Указания по проведению лабораторного практикума

Не предусмотрено учебным планом.

4. Указания по проведению самостоятельной работы студентов

№ п/п	Наименование блока (раздела) дисциплины	Виды СРС
1	Тема 1. Основы защиты информации. Информационная безопасность	Самостоятельное изучение тем Вопросы, выносимые на самостоятельное изучение: 1. Виды и анализ угроз автоматизированных систем. 2. Компьютерные вирусы, технология и способы вторжения в устойчивую работу автоматизированных систем злоумышленников. 3. Уязвимости АС, возможные атаки на них. 4. Модели нарушителей объектов защиты информации.
2	Тема 2. Методы несанкционированного доступа к информационным системам	Самостоятельное изучение тем. Вопросы, выносимые на самостоятельное изучение: 1. Классификация компьютерных систем, подлежащих защите в зависимости от обрабатываемой информации и функционального назначения. 2. Классификация АС по уровню защищённости от НСД к информации. 3. Классификация СВТ по уровню защищённости от НСД к информации. Перечень показателей защищённости СВТ и совокупности описывающих их требований. Характеристика классов защищённости СВТ от НСД к информации. 4. Классификация МЭ по уровню защищённости от НСД к информации.
3	Тема 3. Системный подход к обеспечению безопасности информационных систем	Самостоятельное изучение тем. Вопросы, выносимые на самостоятельное изучение: 1. Анализ зарубежных нормативных документов, связанных с обеспечением информационной безопасности.
4	Тема 4. Комплексная система защиты информации (КСЗИ)	Самостоятельное изучение тем. Вопросы, выносимые на самостоятельное изучение: 1. Анализ нормативных документов ФСТЭК России по вопросам защиты информации 2. Анализ нормативных документов ФСБ России по вопросам защиты информации
5	Тема 5. Проектирование комплексной системы защиты информации (КСЗИ) в ИС	Самостоятельное изучение тем. Вопросы, выносимые на самостоятельное изучение: 1. Структурный принцип и принцип модульного проектирования защищённых АС. Преимущества использования модульного принципа. 2. Этапы разработки защищённой автоматизированной системы (АСЗИ). Процесс создания автоматизированных систем в защищенном исполнении

5. Указания по проведению курсовой работы

Учебным планом предусмотрено выполнение курсовой работы в 6 семестре.

Цель выполнения курсовой работы: на основе проведенного анализа организации разработать элементы системы обеспечения информационной безопасности

Задачи, которые должны быть выполнены в ходе курсовой работы:

- Провести анализ структуры конкретной организации, определить угрозы информационной безопасности и информационные риски, произвести оценку информационных рисков
- Разработать Политику информационной безопасности для конкретной организации
- Разработать совокупность мер защиты информации на процедурном (организационном) и программно-техническом уровнях

Примерные тематики курсовой работы:

1. Разработка элементов системы обеспечения информационной безопасности на примере АО «Мособлгаз»
2. Разработка элементов системы обеспечения информационной безопасности на примере ОО Мосводоканал
3. Разработка элементов системы обеспечения информационной безопасности на примере МУП «Капитальное строительство»
4. Разработка элементов системы обеспечения информационной безопасности на примере ООО СК «Стройград»
5. Разработка элементов системы обеспечения информационной безопасности на примере ООО «СтройГрупп»
6. Разработка элементов системы обеспечения информационной безопасности на примере ООО “ДомКомСтрой”
7. Разработка элементов системы обеспечения информационной безопасности на примере ОАО «Бонолит – строительные решения»
8. Разработка элементов системы обеспечения информационной безопасности на примере Архитектурно-проектная мастерская №1
9. Разработка элементов системы обеспечения информационной безопасности на примере ООО «ГАЗОБЕТОН-24»
10. Разработка элементов системы обеспечения информационной безопасности на примере АО «Специализированное Строительное Управление - 5»
11. Разработка элементов системы обеспечения информационной безопасности на примере ООО «Водосток ЛС»
12. Разработка элементов системы обеспечения информационной безопасности на примере АО «Level Group»

13. Разработка элементов системы обеспечения информационной безопасности на примере ООО «Пластокна»

14. Разработка элементов системы обеспечения информационной безопасности на примере ООО «БКР»

15. Разработка элементов системы обеспечения информационной безопасности на примере ООО “МонтажПромСтрой”

16. Разработка элементов системы обеспечения информационной безопасности на примере ООО «ЭкоСтрой»

17. Разработка элементов системы обеспечения информационной безопасности на примере ГБУ “Гормост”

18. Разработка элементов системы обеспечения информационной безопасности на примере АО «Ренессанс Констракшн»

19. Разработка элементов системы обеспечения информационной безопасности на примере АО «Моспромстрой»

6. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

Основная литература:

1. Бирюков А. Информационная безопасность / А. Бирюков . - Москва : ДМК Пресс, 2017. - с. URL: https://e.lanbook.com/book/93278
2. Рябко Б.Я., Фионов А.Н. Основы современной криптографии и стеганографии – 2-е издание- М.: Горячая линия – Телеком, 2013. – 232с.

Дополнительная литература:

1. Гришина Н.В.Информационная безопасность предприятия : учебное пособие / Н.В. Гришина. - 2-е изд., доп. - М. ; М. : ФОРУМ : НИЦ ИНФРА-М, 2015. - 240 с. - (Высшее образование - бакалавриат)
2. Кияев, В. Безопасность информационных систем / В. Кияев; О. Граничин. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 192 с. URL: http://biblioclub.ru/index.php?page=book&id=429032

7. Перечень ресурсов информационно-телекоммуникационной сети интернет, необходимых для освоения дисциплины (модуля)

12. ISO27000.ru (портал по ИБ, аналитика, информация по законодательству и стандартам, блоги, каталоги ресурсов и ПО).
13. WinSecurity.ru (статьи, документация, новости по безопасности Windows).
14. Журнал Информационная безопасность (публикации, статьи, обзоры, форум).
15. http://www.gov.ru - сервер органов государственной власти Российской Федерации.
16. www.wikIsec.ru - Энциклопедия информационной безопасности. – Публикации, статьи.
17. www.biblioclub.ru - Универсальная библиотека онлайн.

18. www.rucont.ru - ЭБС «Руконт».
19. http://www.minfin.ru - Официальный сайт Министерства финансов Российской Федерации
20. http://www.gov.ru/ - Официальный сервер органов государственной власти Российской Федерации.
21. http://www.fsb.ru/ - Официальный сайт Федеральной Службы Безопасности
22. http://www.fstec.ru/ - Официальный сайт Федеральной Службы по Техническому Экспортному контролю

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

Перечень программного обеспечения: Microsoft Office или свободно распространяемые аналоги, ПО комплекса «Основы компьютерно-информационной безопасности»

Информационные справочные системы:

3. Ресурсы информационно-образовательной среды Технологического университета.
4. Рабочая программа и методическое обеспечение по дисциплине: «Безопасность информационных систем»