Государственное бюджетное образовательное учреждение высшего образования
Московской области

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

имени дважды Героя Советского Союза, летчика-космонавта А.А. Леонова

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ МОСКОВСКОЙ ОБЛАСТИ "ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ ДВАЖДЫ ГЕРОЯ СОВЕТСКОГО СОЮЗА, ЛЕТЧИКА-КОСМОНАВТА А.А.ЛЕОНОВА"

Подписано цифровой подписью: ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ МОСКОВСКОЙ ОБЛАСТИ "ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ ДВАЖДЫ ГЕРОЯ СОВЕТСКОГО СОЮЗА, ЛЕТЧИКА-КОСМОНАВТА А.А.ЛЕОНОВА"

«УТВЕРЖДАЮ»
Проректор по учебно-методической работе
И.В. Бабина
«12» апреля 2022 г.

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РАБОЧАЯ ПРОГРАММА
ДИСЦИПЛИНЫ (МОДУЛЯ)

Б.1.О.12.03 «ОСНОВЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ»

Направление подготовки: 10.03.01 Информационная безопасность
Профиль: Безопасность телекоммуникационных систем (в аэрокосмической сфере)
Уровень высшего образования: бакалавр
Форма обучения: очная

Королев
2022

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: Журавлев С.И. Рабочая программа дисциплины: Основы управления информационной безопасностью. – Королев МО: «Технологический университет», 2022.

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 12.04.2022 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)	2022	2023	2024	2025
Номер и дата протокола заседания кафедры	№8 от 17.03.2022			

Рабочая программа согласована:

Руководитель ОПОП ВО к.т.н., доцент Вихров А.П.

Рабочая программа рекомендована на заседании УМС:

Год утверждения (переутверждения)	2022	2023	2024	2025
Номер и дата протокола заседания УМС	№4 от 12.04.2022			

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

Целью изучения дисциплины является:

1. Дать студентам концептуальные знания основ управления информационной безопасностью для региональных информационных объектов с учетом современных требований теории по защите информации;

2. Выработать и закрепить у студентов базовые умения и навыки по практической организации и реализации современных технологий менеджмента информационной безопасности на типовых региональных информационных объектах с учетом современных международных и отечественных стандартов.

В процессе обучения студент приобретает и совершенствует следующие компетенции.

ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности

ОПК-10. Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты;

Основными **задачами** дисциплины являются:

1. Теоретические основы подготовки студентов в области криптографических методов защиты информации в компьютерных системах и сетях;

2. Практические аспекты формирования подходов к выполнению самостоятельных исследований студентами в области криптографических методов защиты информации в компьютерных системах и сетях.

Показатель освоения компетенции отражают следующие индикаторы:

Необходимые знания:

- знает основы: российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации;
- знает основные понятия и характеристику основных отраслей права, применяемых в профессиональной деятельности организации;
- знает основы законодательства Российской Федерации, нормативные правовые акты, нормативные и методические документы в области информационной безопасности и защиты информации, правовые основы организации защиты государственной тайны и конфиденциальной информации, правовую характеристику преступлений в сфере компьютерной информации и меры правовой и дисциплинарной ответственности за разглашение защищаемой информации;

- знает правовые основы организации защиты персональных данных и охраны результатов интеллектуальной деятельности;
- знает программно-аппаратные средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях
- знает правовые основы организации защиты персональных данных и охраны результатов интеллектуальной деятельности
- знает принципы формирования политики информационной безопасности организации

Необходимые умения:

- умеет обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей, предпринимать необходимые меры по восстановлению нарушенных прав;
- умеет анализировать и разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации;
- умеет формулировать основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации;
- умеет формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации;
- умеет конфигурировать программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Основы управления информационной безопасностью» 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: «Информатика», «Основы информационной безопасности», «Математика», «Информационные процессы и системы как объекты информационной безопасности», «Конфиденциальное делопроизводство и защищенный электронный документооборот» и компетенциях: ОПК-1,2,3,6,7,8,9; ДОПК-1,2,4.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Эффективность

защищенных информационных систем», «Социотехносферная безопасность объектов информационной защиты», «Правовая охрана результатов интеллектуальной деятельности», «Разработка политики информационной безопасности в Интернет-системах», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

3. Объем дисциплины (модуля) и виды учебной работы

Общая трудоемкость дисциплины для студентов очной формы составляет 3 зачетных единицы, 108 часов; для студентов очной формы составляет 3 зачетных единицы, 108 часов.

Таблица1

Виды занятий	**Всего часов**	**Семестр 5**	**Семестр 6**	**Семестр 7**	**Семестр …**
Общая трудоемкость	108	108		108	
ОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	48	48			
Лекции (Л)	16	16			
Практические занятия (ПЗ)	32	32			
Лабораторные работы (ЛР)	-	-			
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	Зачет	Зачет			

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

4.Содержание дисциплины

4.1.Темы дисциплины и виды занятий

Таблица 2

Наименование тем	Лекции, час. Очное	Практические занятия, час	Занятия в интерактивной форме,	Код компетенций

		Очное	час	
Раздел 1. Концептуально-теоретические основы управления информационной безопасностью				
Тема 1. Базовые основы процессов и систем управления информационной безопасностью	4	8	3	ОПК-5
Тема 2. Политика информационной безопасности региона и отдельных региональных структур (объектов, процессов)	4	8	3	ОПК-5
Раздел 2. Прикладные аспекты управления информационной безопасностью				
Тема 3. Организационно-кадровые и технические аспекты управления информационной безопасностью	4	8	3	ОПК-10
Тема 4. Основы оценки эффективности управления информационной безопасностью	4	8	3	ОПК-10
Итого:	**162**	**32**	**12**	

4.2. Содержание тем дисциплины

Раздел 1. Концептуально-теоретические основы управления информационной безопасностью

Тема 1. Базовые основы систем и процессов управления информационной безопасностью

Предмет и задачи курса. Значение и место курса в подготовке магистров по информационной безопасности. Взаимосвязь курса с другими дисциплинами.

Разделы и темы, их распределение по видам аудиторных занятий. Формы проведения контрольных мероприятий. Формы проверки знаний.

Состав и методика самостоятельной работы студентов по изучению дисциплины.

Знания и умения студентов, которые должны быть получены в результате изучения курса. Рекомендованная научная и учебная литература.

Характеристика базовой терминологии в области управления информационной безопасностью: сущность управления; управление как процесс; системный подход к управлению; процессный подход к управлению; циклическая модель улучшения процессов управления; системы управления информационной безопасностью.

Стандартизация систем и процессов управления информационной безопасностью: международные и российские стандарты; особенности стандартов банковской системы РФ.

Тема 2. Политика информационной безопасности отдельных региональных структур (объектов, процессов)

Понятие политики обеспечения информационной безопасности региона и политики информационной безопасности организаций (учреждений и предприятий). Причина выработки политики информационной безопасности. Основные требования и принципы, учитываемые при разработке и внедрении информационной безопасности. Содержание корпоративной и частных политик информационной безопасности.

Жизненный цикл политик информационной безопасности: разработка; внедрение; применение и аннулирование. Ответственность за исполнение политики информационной безопасности.

Раздел 2. Прикладные аспекты управления информационной безопасностью

Тема 3. Организационно-кадровые и технические аспекты управления информационной безопасностью

Особенности организации управления информационной безопасностью региона: корпоративных структур, отдельных организаций и их информационно- телекоммуникационных технологий.

Организация реагирования на чрезвычайные ситуации (инциденты). Управления информационными рисками. Аудит (мониторинг) состояния информационной безопасности региона. Стратегии построения и внедрения управленческих процессов и систем управления информационной безопасностью в целом.

Система управления информационной безопасностью: область действия; документальное обеспечение; политика системы управления и поддержка системы управления со стороны руководства. Основы

кадрового обеспечения управления информационной безопасностью. Департамент информационной безопасности региона.

Технические аспекты управления информационной безопасностью. Администрирование информационных систем управления информационной безопасностью. Защита систем управления информационной безопасностью региона.

Страхование информационных рисков: основы методологии и рынок страховых услуг. Методические основы экономики информационной безопасности

Тема 4. Основы оценки эффективности управления информационной безопасностью

Нормативное обеспечение проверки и оценки деятельности по управлению информационной безопасностью: международные и российские стандарты.

Характеристики типовых процессов проверки систем управления информационной безопасности: виды проверок, мониторинг, самооценка, внутренний и внешний аудит, инструментальные средства.

Практическая оценка деятельности по управлению информационной безопасности: результативность (эффективность), метрики и измерения, модели зрелости процессов систем управления информационной безопасностью.

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 «Основы управления информационной безопасностью» приведена в Приложении 1.

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

Основная литература:

1. Гришина Н. В. Информационная безопасность предприятия: Учебное пособие / Гришина Наталия Васильевна. - 2; доп. - Москва; Москва: Издательство "ФОРУМ": ООО "Научно-издательский центр ИНФРА-М", 2015. - 240 с. - ДЛЯ СТУДЕНТОВ ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЙ. - ISBN 978-5-00091-007-8. URL: http://znanium.com/go.php?id=491597.

2.Малюк А. А. Теория защиты информации [Текст] / А. А. Малюк. - М.: Горячая линия - Телеком, 2013. - 184 с.: ил. - (Научное издание). - ISBN 978-5-9912-0246-6.

Дополнительная литература:

3.Шишов О. В. Технические средства автоматизации и управления: учебное пособие / О.В. Шишов. — Москва: ИНФРА-М, 2021. — 396 с. + Доп. материалы [Электронный ресурс]. — (высшее образование: Бакалавриат). - ISBN 978-5-16-010325-9. - Текст: электронный. - URL: https://znanium.com/catalog/product157118

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. **http://www.academy.it.ru/ –** академия АЙТИ.

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, PowerPoint.

- **Информационные справочные системы:**

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

Ресурсы информационно-образовательной среды МГОТУ:
Рабочая программа и методическое обеспечение по курсу «Основы управления информационной безопасностью»

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 ТЕХНИКИ И ЦИФРОВЫХ ТЕХНОЛОГИЙ

ФАКУЛЬТЕТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

«ОСНОВЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ»

(Приложение 1 к рабочей программе)

Направление подготовки: 10.03.01 Информационная безопасность
Профиль: Безопасность телекоммуникационных систем (в аэрокосмической сфере)
Уровень высшего образования: бакалавр
Форма обучения: очная

Королев
2022

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

№ п/п	Индекс компетенции	Содержание компетенции	Раздел дисциплины, обеспечивающий формирование компетенции	В результате изучения раздела дисциплины, обеспечивающего формирование компетенции, обучающийся приобретает:		
				Трудовые действия	Необходимые умения	Необходимые знания
1.	ОПК-5	Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности;	Тема:1,4		- умеет обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей, предпринимать необходимые меры по восстановлению нарушенных прав; - умеет анализировать и разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечени	- знает основы: российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации; - знает основные понятия и характеристику основных отраслей права, применяемых в профессиональной деятельности организации; - знает основы законодательства Российской Федерации, нормативные правовые акты, нормативные и методические документы в области информационной безопасности и защиты информации, правовые основы организации защиты государственной

					ю информационной безопасности в организации; - умеет формулировать основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации; - умеет формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации;	тайны и конфиденциальной информации, правовую характеристику преступлений в сфере компьютерной информации и меры правовой и дисциплинарной ответственности за разглашение защищаемой информации; - знает правовые основы организации защиты персональных данных и охраны результатов интеллектуальной деятельности;
2.	ОПК-10	Способен в качестве технического	Тема:1,2,3		- умеет конфигурировать	- знает программно-аппаратные

		специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты;			программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности	средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях - знает правовые основы организации защиты персональных данных и охраны результатов интеллектуальной деятельности - знает принципы формирования политики информационной безопасности организации

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*
ОПК-5,10	***Доклад***	***А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 5 баллов*** ***Б) частично сформирована:*** • ***компетенция освоена на <u>продвинутом</u> уровне – 4 балла;*** • ***компетенция освоена на <u>базовом</u> уровне – 3 балла;*** ***В) не сформирована (<u>компетенция не сформирована</u>) – 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.***
ОПК-5,10	***Выполнение контрольной работы***	***А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 5 баллов*** ***Б) частично сформирована:*** • ***компетенция освоена на <u>продвинутом</u> уровне – 4 балла;*** • ***компетенция освоена на <u>базовом</u> уровне – 3 балла;*** ***В) не сформирована (<u>компетенция не</u>***	***При определении сформированности компетенций критериями оценивания выступают методические рекомендации, разработанные по дисциплине для данного вида***

		сформирована) – 2 и менее баллов	

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 форме презентации:

1. Ведущие мировые разведки и их деятельность в России.
2. Основы обеспечения безопасности информации в компьютерных системах.
3. Информационная безопасность современной России: угрозы и их отражения.
4. Информационные войны в современном мире.
2. Компьютерная преступность в экономических областях.
3. Мир XXI века: информационное противоборство.
4. Компьютерные вирусы в современных информационных системах.
5. Информационные угрозы современным экономическим объектам.
6. Информатизация России и проблема защиты информации.
7. Безопасность информации в коммерческой деятельности.
8. Разведки России – исторический аспект.
9. Мировой информационный терроризм.
10. Этика защиты информации.
11. Становление и развитие промышленного шпионажа.

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

Формой контроля знаний по дисциплине «Основы управления информационной безопасностью» являются две текущие аттестации в виде тестов и итоговая аттестация в виде зачета.

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	ОПК-5,10	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%.***
Проводится в сроки, установленные графиком образовательного процесса	тестирование	ОПК-5,10	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%.***
Проводится в сроки, установленные графиком образовательного процесса	Зачет	ОПК-5,10	3 вопроса	Зачет проводится в письменной форме, путем ответа на вопросы. Время, отведенное на процедуру – 30 минут.	Результаты предоставляются в день проведения зачета	Критерии оценки: **«Зачтено»:** – знание основных понятий предмета; – умение использовать и применять полученные

						знания на практике; – работа на семинарских занятиях; – знание основных научных теорий, изучаемых предметов; – ответ на вопросы билета. **«Не зачтено»:** – демонстрирует частичные знания по темам дисциплин; – незнание основных понятий предмета; – неумение использовать и применять полученные знания на практике; – не работал на семинарских занятиях; – не отвечает на вопросы.

Примерное содержание тестов для текущей аттестации:

ЗАДАНИЕ НА ВЫБОР ОДНОГО ПРАВИЛЬНОГО ВАРИАНТА ОТВЕТА

1. Требование безопасности повторного использования объектов противоречит:
инкапсуляции +

наследованию
полиморфизму
2. Предположим, что при разграничении доступа учитывается семантика программ. В таком случае на игровую программу могут быть наложены следующие ограничения:
запрет на чтение каких-либо файлов, кроме конфигурационных
запрет на изменение каких-либо файлов, кроме конфигурационных +
запрет на установление сетевых соединений
3. В число граней, позволяющих структурировать средства достижения информационной безопасности, входят:
меры обеспечения целостности
административные меры +
меры административного воздействия
4. Дублирование сообщений является угрозой:
доступности
конфиденциальности
целостности +
5. Самыми опасными источниками внутренних угроз являются:
некомпетентные руководители +
обиженные сотрудники
любопытные администраторы
6. Для внедрения бомб чаще всего используются ошибки типа:
отсутствие проверок кодов возврата
переполнение буфера +
нарушение целостности транзакций
7. В число целей политики безопасности верхнего уровня входят:
решение сформировать или пересмотреть комплексную программу безопасности +
обеспечение базы для соблюдения законов и правил +
обеспечение конфиденциальности почтовых сообщений
8. В число целей программы безопасности верхнего уровня входят:
управление рисками +
определение ответственных за информационные сервисы
определение мер наказания за нарушения политики безопасности
9. В рамках программы безопасности нижнего уровня осуществляются:
стратегическое планирование
повседневное администрирование +
отслеживание слабых мест защиты +
10. Политика безопасности строится на основе:
общих представлений об ИС организации
изучения политик родственных организаций
анализа рисков +
11. В число целей политики безопасности верхнего уровня входят:
формулировка административных решений по важнейшим аспектам

реализации программы безопасности +
выбор методов аутентификации пользователей
обеспечение базы для соблюдения законов и правил +

Типовые вопросы, выносимые на зачет

1. Процессный подход к построению СУИБ и циклическая модель PDCA.
2. Цели и задачи, решаемые СУИБ.
3. Стандартизация в области построения СУИБ: сходства и различия стандартов.
4. Стратегии выбора области деятельности СУИБ.
5. Стратегии построения СУИБ (построение системы в целом, построение отдельных процессов управления ИБ с последующим объединением в систему).
6. Основные этапы разработки СУИБ и роль руководства организации на каждом из этапов.
7. Политика ИБ и политика СУИБ: сходства и различия.
8. Распределение ролей и ответственности в рамках СУИБ: базовая ролевая структура, дополнительные роли в рамках процессов управления ИБ.
9. Анализ рисков ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
10. Анализ рисков ИБ: основные подходы, основные этапы процесса.
11. Управление инцидентами ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
12. Расследование инцидентов ИБ: виды расследования инцидентов, критерии выбора необходимого вида расследования, основные этапы расследования (для различных видов расследования).
13. Внутренние аудиты ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
14. Анализ со стороны руководства: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
15. Обучение и обеспечение осведомленности пользователей: цели и задачи процесса, роль процесса в рамках СУИБ.
16. Внедрение процессов управления ИБ: этапы и последовательность. Ввод СУИБ в эксплуатацию: возможные проблемы и способы их решения
17. Правовые аспекты построения СУИБ организации.

**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)

«ОСНОВЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ»

Направление подготовки: 10.03.01 Информационная безопасность
Профиль: Безопасность телекоммуникационных систем (в аэрокосмической сфере)
Уровень высшего образования: бакалавр
Форма обучения: очная

Королев
2022

1. Общие положения

Целями изучения дисциплины является:

– Дать студентам концептуальные знания основ управления информационной безопасностью для региональных информационных объектов с учетом современных требований теории по защите информации;

– Выработать и закрепить у студентов базовые умения и навыки по практической организации и реализации современных технологий менеджмента информационной безопасности на типовых региональных информационных объектах с учетом современных международных и отечественных стандартов.

Задачами дисциплины являются:

1. Ознакомление обучаемых с основными методами управления.
2. Изучение правовых, организационных и программно-технических мер обеспечения информационной безопасности.
3. Формирование у обучаемых понимания роли процессов управления в обеспечении информационной безопасности организаций, объектов и систем
4. Формирование требований к системе управления ИБ конкретного объекта
5. Обучение различным методам реализации процессов управления информационной безопасностью, направленных на эффективное управление ИБ конкретной организации
6. Проектирование системы управления ИБ конкретного объекта.

2. Указания по проведению практических занятий

Раздел 1. Концептуально-теоретические основы управления информационной безопасностью

Тема 1. Базовые основы систем и процессов управления информационной безопасностью

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: Получить практические знания и навыки систем и процессов управления информационной безопасностью

Учебные вопросы:

- Управление информационной безопасностью. Комплексная система управления информационной безопасностью.
- Основные определения и критерии классификации угроз. Основные угрозы доступности.
- Основные угрозы целостности.
- Основные угрозы конфиденциальности.
- Источники угроз.

Продолжительность занятия – 8 ч.

Тема 2. Политика информационной безопасности отдельных структур (объектов, процессов)

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: Получить практические знания и навыки о политике безопасности отдельных структур

Учебные вопросы:

- Определение политики информационной безопасности
- Принципы политики безопасности
- Виды политики безопасности
- Политики безопасности для
- Уровни политики безопасности

Продолжительность занятия – 8 ч.

Раздел 2. Прикладные аспекты управления информационной безопасностью

Тема 3. Организационно-кадровые и технические аспекты управления информационной безопасностью

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: Получить практические знания и навыки в организационно-кадровых и технических аспектах управления информационной безопасностью

Учебные вопросы:

- Основные направления обеспечения информационной безопасности. Законодательно-правовая база обеспечения информационной безопасности на предприятии.
- Нормативные акты предприятия по информационной безопасности.
- Формы правовой защиты информации на предприятии.

Продолжительность занятия – 8 ч.

Тема 4. Основы оценки эффективности управления информационной безопасностью

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 практические знания и навыки оценки эффективности управления ИБ

Учебные вопросы:

- Метод оценки рисков на основе модели информационных потоков.
- Расчет рисков по угрозе конфиденциальность.
- Расчет рисков по угрозе целостность.
- Методы оценивания информационных рисков.
- Табличные методы оценки рисков.
- Разделение рисков на приемлемые и неприемлемые.

Продолжительность занятия – 8 ч.

4. Указания по проведению самостоятельной работы студентов

№ п/п	Наименование блока (раздела) дисциплины	Виды СРС
1.	**Тема 1. Базовые основы процессов и систем управления информационной безопасностью**	***Подготовка докладов по темам:*** 1. Место информационной безопасности в системе национальной безопасности. 2. Современная концепция информационной безопасности. 3. Цели и концептуальные основы защиты информации. 4. Критерии, условия и принципы отнесения информации к защищаемой. 5. Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности.

		6. Понятие и структура угроз защищаемой информации. 7. Источники, виды и методы дестабилизирующего воздействия на защищаемую информацию. 8. Причины, обстоятельства и условия, вызывающие
2.	**Тема 2. Политика информационной безопасности региона и отдельных региональных структур (объектов, процессов)**	***Подготовка докладов по темам:*** 9. Виды уязвимости информации и формы ее проявления. 10. Каналы и методы несанкционированного доступа к конфиденциальной информации. 11. Модель нарушителя. 12. Модель угроз. 13. Критерии оценки безопасности информационных технологий. 14. Методы защиты информации от несанкционированного доступа. 15. Риски информационной безопасности.
3	**Тема 3. Организационно-кадровые и технические аспекты управления информационной безопасностью**	***Подготовка докладов по темам:*** 1. Вредоносные программы и антивирусные программные средства. 2. Методы программно-аппаратной защиты информации. 3. Аттестация объектов информатизации. 19. Виды защиты информации. 4. Системы защиты информации. 5. Модели разграничения доступа. 6. Криптографические стандарты и их использование в информационных системах. 7. Способы и средства защиты информации от утечки по техническим каналам.
4	**Тема 4. Основы оценки эффективности управления информационной безопасностью**	***Подготовка докладов по темам:*** 8. Принципы организации информационных систем в соответствии с требованиями по защите информации. 9. Основные нормативные правовые акты в области информационной безопасности и защиты информации. 10. Отечественные и зарубежные стандарты в области компьютерной безопасности. 11. Принципы и методы организационной защиты информации. 12. Методы и средства обнаружения уязвимостей

		в корпоративных компьютерных сетях. 13. Лицензирование и сертификация в области защиты информации. 14. Комплексные системы защиты информации.

5. Указания по проведению контрольных работ

5.1. 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: Типовые вопросы, выносимые на зачет

1. Процессный подход к построению СУИБ и циклическая модель PDCA.
2. Цели и задачи, решаемые СУИБ.

3. Стандартизация в области построения СУИБ: сходства и различия стандартов.
4. Стратегии выбора области деятельности СУИБ.
5. Стратегии построения СУИБ (построение системы в целом, построение отдельных процессов управления ИБ с последующим объединением в систему).
6. Основные этапы разработки СУИБ и роль руководства организации на каждом из этапов.
7. Политика ИБ и политика СУИБ: сходства и различия.
8. Распределение ролей и ответственности в рамках СУИБ: базовая ролевая структура, дополнительные роли в рамках процессов управления ИБ.
9. Анализ рисков ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
10. Анализ рисков ИБ: основные подходы, основные этапы процесса.
11. Управление инцидентами ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
12. Расследование инцидентов ИБ: виды расследования инцидентов, критерии выбора необходимого вида расследования, основные этапы расследования (для различных видов расследования).
13. Внутренние аудиты ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
14. Анализ со стороны руководства: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
15. Обучение и обеспечение осведомленности пользователей: цели и задачи процесса, роль процесса в рамках СУИБ.
16. Внедрение процессов управления ИБ: этапы и последовательность. Ввод СУИБ в эксплуатацию: возможные проблемы и способы их решения
17. Правовые аспекты построения СУИБ организации.

6. Перечень основной и дополнительной учебной литературы

Основная литература:

1. Гришина Н. В. Информационная безопасность предприятия: Учебное пособие / Гришина Наталия Васильевна. - 2; доп. - Москва; Москва: Издательство "ФОРУМ": ООО "Научно-издательский центр ИНФРА-М", 2015. - 240 с. - ДЛЯ СТУДЕНТОВ ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЙ. - ISBN 978-5-00091-007-8. URL: http://znanium.com/go.php?id=491597.
2.Малюк А. А. Теория защиты информации [Текст] / А. А. Малюк. - М.: Горячая линия - Телеком, 2013. - 184 с.: ил. - (Научное издание). - ISBN 978-5-9912-0246-6.

Дополнительная литература:

3.Шишов О. В. Технические средства автоматизации и управления: учебное пособие / О.В. Шишов. — Москва: ИНФРА-М, 2021. — 396 с. + Доп. материалы [Электронный ресурс]. — (высшее образование: Бакалавриат). -

ISBN 978-5-16-010325-9. - Текст: электронный. - URL: https://znanium.com/catalog/product157118

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

Перечень программного обеспечения: *MSOffice, Multisim.*

Информационные справочные системы:

1. Электронные ресурсы образовательной среды Университета
2. Информационно-справочные системы (Консультант+; Гарант).
3. Рабочая программа и методическое обеспечение по курсу «Основы управления информационной безопасностью»