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

УТВЕРЖДАЮ
И.о. проректора
_____ А.В. Троицкий
«___»_____2023г.

Троицкий Александр Витальевич
Подписано цифровой подписью: Троицкий Александр Витальевич

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ
КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РАБОЧАЯ ПРОГРАММА
ДИСЦИПЛИНЫ
«ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Направление подготовки: 01.03.02. Прикладная математика и информатика

Профиль: Программирование, математическое моделирование

Уровень высшего образования: бакалавриат

Форма обучения: очная

Королев
2023

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

Автор: преподаватель Ульянов Д.В. Рабочая программа дисциплины: «Основы информационной безопасности». – Королев МО: «Технологический университет», 2023.

Рецензент: **к.в.н., доцент Сухотерин А.И.**

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки бакалавров 01.03.02 «Прикладная математика и информатика» и Учебного плана, утвержденного Ученым советом Университета. Протокол № 9 от 11.04.2023 г.

Рабочая программа рассмотрена и одобрена на заседании кафедры:

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

Рабочая программа согласована:

Руководитель ОПОП ВО_____ И.В. Бугай, к.т.н., доцент

Рабочая программа рекомендована на заседании УМС:

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

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

Целью изучения дисциплины формирование у студентов специализированной базы знаний по фундаментальным проблемам информационной безопасности в условиях становления современного информационного общества, в использовании организационно-технических механизмов обеспечения защиты информационных объектов, а также получение навыков в применении технологий обеспечения информационной безопасности для защищаемых объектов.

В процессе обучения студент приобретает и совершенствует следующие компетенции:

профессиональные компетенции (ПК):

- Способность учитывать знания проблем и тенденций развития рынка ПО в профессиональной деятельности (ПК-4);

универсальные компетенции (УК):

Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений (УК-2).

Основными задачами дисциплины являются:

1. Ознакомление студентов с методологическими подходами применения и эксплуатации основных технических средств информационной безопасности защищаемых объектов, а также с основными методами определения параметров, характеристик и условий применения технических средств защиты на основе анализа возможных угроз информационной безопасности и потенциальных каналов утечки информации;
2. Формирование у студентов способности самостоятельно решать поставленные задачи в области информационной безопасности с помощью существующих принципов, методов и технологий в различных организационных структурах, по базовым направлениям и применительно к типовым информационным объектам.

Показатель освоения компетенции отражают следующие индикаторы:

Необходимые знания:

- Формулирует проблему, решение которой напрямую связано с достижением цели проекта;
- Анализирует план-график реализации проекта в целом и выбирает способ решения поставленных задач
- Знать возможности существующей программно-технической архитектуры
- Знать возможности современных и перспективных средств разработки программных продуктов, технических средств

- Знать методологии разработки программного обеспечения и технологии программирования
- Знать методологии и технологии проектирования и использования баз данных.

Необходимые умения:

- Определяет связи между поставленными задачами и ожидаемые результаты их решения;
- В рамках поставленных задач определяет имеющиеся ресурсы и ограничения, действующие правовые нормы
- Уметь проводить анализ исполнения требований
- Уметь вырабатывать варианты реализации требований.

Трудовые действия:

- Оценивает решение поставленных задач в зоне своей ответственности в соответствии с запланированными результатами контроля, при необходимости корректирует способы решения задач
- Проводить оценку и обоснование рекомендуемых решений
- Осуществлять коммуникации с заинтересованными сторонами.

2. Место дисциплины в структуре ОПОП

Дисциплина «Основы информационной безопасности» относится к обязательной части основной профессиональной образовательной программы подготовки бакалавров по направлению подготовки 01.03.02. «Прикладная математика и информатика».

Дисциплина базируется на ранее изученных дисциплинах: «Архитектура вычислительных систем», «Операционные системы, среды и оболочки», «Системы управления БД», «Правовые основы рынка ПО», «Технологии и среды программирования», «Правовые основы социального обеспечения инвалидов и лиц с ОВЗ», «Адаптированные информационные технологии» и компетенциях: УК-2, ОПК-4, ОПК-5, ПК-1, ПК-2, ПК-4, ПК-5.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми при выполнении выпускной квалификационной работы бакалавра.

3. Объем дисциплины и виды учебной работы

Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы, 108 часов. Практическая подготовка обучающихся составляет 16 часов.

Таблица 1

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

Практическая подготовка	**16**		16		
Самостоятельная работа	**60**		**60**		
Курсовые работы (проекты)	-		-		
Расчетно-графические работы					
Контрольная работа	+		+		
Текущий контроль знаний	Тест		Тест		
Вид итогового контроля	зачет		зачет		
ЗАОЧНАЯ ФОРМА НЕ ПРЕДУСМОТРЕНА УЧЕБНЫМ ПЛАНОМ					

4. Содержание дисциплины

4.1. Темы дисциплины и виды занятий

Таблица 2

Наименование тем	Лекции, час.	Практические занятия, час	Лабораторные занятия, час	Занятия в интерактивной форме, час	Практическая подготовка	Код компетенций
Тема 1. Концепция информационной безопасности.	2	4	-	-	-	ПК – 4 УК – 2
Тема 2. Основные направления обеспечения информационной безопасности.	2	4	-	1	2	ПК – 4 УК – 2
Тема 3. Основные способы защиты информации.	2	4	-	2	2	ПК – 4 УК – 2
Тема 4. Защита информации от утечки по техническим каналам связи.	2	4	-	2	2	ПК – 4 УК – 2
Тема 5. Способы противодействия несанкционированному доступу к источникам конфиденциальной информации.	2	4	-	2	4	ПК – 4 УК – 2
Тема 6. Особенности защиты информационных объектов с помощью технических средств.	2	4	-	2	2	ПК – 4 УК – 2
Тема 7. Защитные меры при работе с зарубежными партнёрами.	2	4	-	1	2	ПК – 4 УК – 2
Тема 8. Методика разработки системы защиты информации на предприятии.	2	4	-	2	2	ПК – 4 УК – 2
Итого:	**16**	**32**	**-**	**12**	**16**	

4.2 Содержание тем дисциплины

Тема 1. Концепция информационной безопасности.

Основные концептуальные положения системы информационной безопасности. Понятие информации и три подхода к определению информации. Определение системы информационной безопасности и требования к ней. Основные виды обеспечения информационной безопасности и системы защиты информации. Концептуальная модель информационной безопасности, её состав и особенности применения. Характеристика действий, приводящих к неправомерному овладению конфиденциальной информацией.

Тема 2. Основные направления обеспечения информационной безопасности.

Характеристика направлений информационной безопасности и перечень защитных действий. Особенности правовой защиты информации. Структура законодательства РФ в области информационной безопасности и защиты информации. Понятие конфиденциальной информации и виды тайн в Российском законодательстве. Основные определения, состав и особенности реализации организационной защиты информации. Предназначение, состав и основные задачи службы безопасности предприятия, фирмы. Предназначение, состав и особенности реализации инженерно-технической защиты информационных объектов.

Тема 3. Основные способы защиты информации.

Понятие способа защиты информации и состав основных организационных и технических мероприятий по её защите. Чем достигается обеспечение информационной безопасности, основные цели защиты информации. Каналы распространения информации и порядок реализации защитных действий от неправомерного овладения конфиденциальной информацией. Матрица, характеризующая взаимосвязь источников информации, целей защиты и механизмов защиты в процессе телекоммуникационного обмена сведениями.

Тема 4. Защита информации от утечки по техническим каналам связи.

Определение утечки информации и способы её классификации. Структура канала утечки информации и классификация технических каналов. Классификация и особенности проявления визуально-оптических каналов утечки информации и особенности защиты информации по ним. Классификация и особенности проявления акустических каналов утечки информации и особенности защиты информации по ним. Классификация и особенности проявления электромагнитных каналов утечки информации и особенности защиты информации по ним. Характеристика применяемых средств защиты информации от утечки по различным каналам.

Тема 5. Способы противодействия несанкционированному доступу к источникам конфиденциальной информации.

Характеристика основных способов несанкционированного доступа к информации. Состав обобщённой модели способов несанкционированного доступа к источникам конфиденциальной информации и их взаимосвязь друг с другом. Обзор и основные возможности технических средств несанкционированного доступа к информации. Порядок контроля и прослушивания телефонных каналов связи, методика непосредственного подключения к телефонной линии. Особенности перехвата компьютерной

информации и несанкционированного внедрения в базы и банки данных. Применение скрытой фото- и видеосъёмки при помощи специальной оптики.

Тема 6. Особенности защиты информационных объектов с помощью технических средств.

Понятие, классификация и особенности применения акустических систем радиоподслушивания (радиозакладок), их параметры и характеристики. Обзор и классификация основных средств обнаружения радиосигналов. Предназначение, состав, основные характеристики и возможности индикаторов поля, панорамных радиоприёмников, сканеров и нелинейных радиолокаторов, порядок их применения и примеры. Понятие радиоэлектронных помех, их разновидности и порядок постановки. Методика обеспечения безопасности телефонных переговоров и противодействия лазерному подслушиванию с помощью специальных технических средств.

Тема 7. Защитные меры при работе с зарубежными партнёрами.

Основные направления взаимодействия с зарубежными партнёрами и порядок организации научно-технического сотрудничества с ними. Вопросы защиты интеллектуальной собственности в соглашениях и договорах о международном сотрудничестве. Технологический обмен результатами совместной деятельности и порядок его регулирования. Структура рынка по реализации новых технологий, характеристика основных путей технологического обмена между странами. Основные виды международных коммерческих операций и их характеристика. Анализ возможных условий разглашения сведений, составляющих коммерческую тайну и научно-техническая документация как источник конфиденциальной информации в международных сделках. Организация безопасной работы с зарубежными партнёрами.

Тема 8. Методика разработки системы защиты информации на предприятии.

Общепринятая методика проведения аудита выделенных помещений и её особенности. Возможности специального оборудования и технических средств, рекомендованных для проведения аудита. Состав итоговых документов по результатам аудита и их оценка. Порядок разработки системы защиты информации на предприятии, характеристика основных стадий разработки и этапов работы. Общий порядок действий по обеспечению информационной безопасности на основных этапах разработки системы. Полномочия специальной приёмной комиссии, её состав и итоговые документы по приёму разработанной или усовершенствованной системы защиты информационных объектов на предприятии.

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

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

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

Структура фонда оценочных средств приведена в Приложении 1.

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

Основная литература:

1. Информационная безопасность предприятия: Учебное пособие / Н.В. Гришина. - 2-е изд., доп. - М.: Форум: НИЦ ИНФРА-М, 2015. - 240 с.: ил.; 60x90 1/16. - (Высшее образование: Бакалавриат). (обложка) ISBN 978-5-00091-007-8http://znanium.com/bookread2.php?book=491597

2. Загинайлов Ю.Н. Основы информационной безопасности: курс визуальных лекций : учебное пособие / Ю.Н. Загинайлов. - М. ; Берлин : Директ-Медиа, 2015. - 105 с. : ил. - Библиогр. в кн. - ISBN 978-5-4475-3947-4 ; То же [Электронный ресурс]. - URL://biblioclub.ru/index.php?page=book&id=362895

3. Информационная безопасность: учебное пособие под общ. редакцией проф. Ясенева В.Н.; Министерство образования и науки Российской Федерации, Национальный исследовательский Нижегородский государственный университет им. Н.И. Лобачевского - Нижний Новгород, 2017. - 198 с. : УДК 311(075.8) ББК У051; [Электронный ресурс]:
http://www.iee.unn.ru/wp-content/uploads/sites/9/2014/09/Uchebnoe-posobie-po-IB-pod-redaktsiej-YAseneva-V.N.-2017.pdf

4. 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:

1. Е.В. Вострецова Основы информационной безопасности; Учебное пособие; Министерство образования и науки Российской Федерации, Уральский федеральный университет, Екатеринбург, Издательство Уральского университета 2019; 204 с., ISBN 978-5-7996-2677-8, https://elar.urfu.ru/bitstream/10995/73899/3/978-5-7996-2677-8_2019.pdf

2. Безопасность объектов критической информационной инфраструктуры организации. Общие рекомендации (версия 1.0); АРСИБ, Москва 2019, http://aciso.ru/news/3948/

3. А. Першин, Безопасность мобильных технологий в корпоративном секторе. Общие рекомендации (версия 2.0); АРСИБ, Москва 2016, http://aciso.ru/news/3901/

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

Интернет-ресурсы:

1. http://eup.ru – научно - образовательный портал.
2. http://znanium.com – образовательный портал
3. http://www.academy.it – академия АЙТИ

8. Методические указания для обучающихся по освоению дисциплины

Методические указания для обучающихся по освоению дисциплины 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:

1. Ресурсы информационно-образовательной среды МГОТУ;
2. Информационно – справочные (правовые) системы: «Консультант +».

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 лекции в форме слайд-презентации, оборудованный современными лицензионными программно-техническими средствами: операционная система не ниже Windows 7, офисные программы MSOffice;

- рабочее место преподавателя, оснащенное компьютером с доступом в глобальную сеть Интернет;

- рабочие места студентов, оснащенные компьютерами с доступом в глобальную сеть Интернет.

Приложение 1

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ
КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ «ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Направление подготовки: 01.03.02 Прикладная математика и информатика

Профиль: Программирование, математическое моделирование

Уровень высшего образования: бакалавриат

Форма обучения: очная

Королев
2023

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

№ п/п	Индекс компетенции	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:		
				Необходимые знания	Необходимые умения	Трудовые действия
1.	УК-2	Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	Тема1. - 8.	Формулирует проблему, решение которой напрямую связано с достижением цели проекта; Анализирует план-график реализации проекта в целом и выбирает способ решения поставленных задач	Определяет связи между поставленными задачами и ожидаемые результаты их решения; В рамках поставленных задач определяет имеющиеся ресурсы и ограничения, действующие правовые нормы	Оценивает решение поставленных задач в зоне своей ответственности в соответствии с запланированными результатами контроля, при необходимости корректирует способы решения задач
2.	ПК-4	Способность учитывать знания проблем и тенденций развития рынка ПО в профессиональной деятельности	Тема 1. - 8.	Знать возможности существующей программно-технической архитектуры Знать возможности современных и перспективных средств разработки программных продуктов, технических средств Знать методологии разработки программного обеспечения и технологии программирования Знать методологии и технологии проектирования и использования баз данных	Уметь проводить анализ исполнения требований Уметь вырабатывать варианты реализации требований	Проводить оценку и обоснование рекомендуемых решений Осуществлять коммуникации с заинтересованными сторонами

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

Код компетенции	Инструменты, оценивающие сформированность компетенции	Этапы и показатель оценивания компетенции	Шкала и критерии оценки
УК-2, ПК-4	Тест	А) **полностью сформирована** (компетенция освоена на высоком уровне) – 90% правильных ответов Б) **частично сформирована**: •компетенция **освоена на продвинутом уровне** – 70% правильных ответов; •**компетенция освоена на базовом уровне** – от 51% правильных ответов; В) **не сформирована** (компетенция не освоена) – менее 50% правильных ответов	Проводится письменно Время, отведенное на процедуру –45 мин. Неявка 0 баллов. Критерии оценки определяются процентным соотношением. Неудовлетворительно – менее 50% правильных ответов. Удовлетворительно – от 51% правильных ответов. Хорошо – от 70%. Отлично – от 90%. Максимальная оценка – 5 баллов.
ПК-4	Доклад в форме презентации	А) полностью сформирована **5 баллов** В) частично сформирована **3-4 балла** С) не сформирована **2 балла**	Проводится устно с использованием мультимедийных систем, а также с использованием технических средств Время, отведенное на процедуру – 10 - 15 мин. Неявка – 0. Критерии оценки: 1.Соответствие представленной презентации заявленной тематике (1 балл). 2.Качество источников и их количество при подготовке доклада и разработке презентации (1 балл). 3.Владение информацией и способность отвечать на вопросы аудитории (1 балл). 4.Качество самой представленной презентации (1 балл). 5.Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл). 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.
УК-2	Реферат	А) полностью сформирована **5 баллов** В) частично	Проводится в письменной форме Критерии оценки: 1. Соответствие содержания реферата заявленной тематике (1

		сформирована **3-4 балла** С) не сформирована **2 балла**	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. Результаты оценочной процедуры представляются обучающимся в срок не позднее 1 недели после проведения процедуры – для текущего контроля. Оценка проставляется в электронный журнал.
УК-2 ПК-4	Выполнение контрольной работы	А) **полностью сформирована** (компетенция освоена на высоком уровне) – 5 баллов Б) **частично сформирована**: •компетенция **освоена на продвинутом уровне** – 4 балла; •**компетенция освоена на базовом уровне** – 3 балла; В) **не сформирована** (компетенция не освоена) – 2 и менее баллов	При определении сформированности компетенций критериями оценивания выступают методические рекомендации, разработанные по дисциплине для данного вида.

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

Типовая тематика докладов в презентационной форме:

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.
5. Компьютерная преступность в экономических областях.
6. Мир XXI века: информационное противоборство.
7. Компьютерные вирусы в современных информационных системах.
8. Информационные угрозы современным экономическим объектам.

9. Информатизация России и проблема защиты информации.
10. Безопасность информации в коммерческой деятельности.
11. Мировой информационный терроризм.
12. Становление и развитие промышленного шпионажа.

Тематика рефератов:

1. Программы компьютерного слежения и радиоэлектронной разведки в США, Великобритании, КНР и других странах.
2. Информационное общество и проблема его безопасности.
3. Российская экономика и ее информационная безопасность.
4. ФСТЭК и ФСБ как регуляторы деятельности в области информационной безопасности.
5. Защита информации в деятельности государственного предприятия.
6. Вопросы информационной безопасности в критической информационной инфраструктуре (КИИ) - нормативные документы, терминология и технологические решения.
7. Правовая основа защиты информации в России.
8. Банки в электронную эпоху и их информационная безопасность.
9. Организационные мероприятия по информационной безопасности.
10. Информационная безопасность в ведущих зарубежных странах.
11. Инженерно – техническая защита информации как базовое направление обеспечения информационной безопасности.
12. Криптографическая защита информации в современных информационных технологиях.
13. Современная доктрина информационной безопасности России.
14. Современные информационные системы и технологии управления и обеспечение их безопасности.
15. Система безопасности предприятия и роль службы защиты информации.
16. Безопасность электронного бизнеса.
17. Квантовые компьютеры. Разработки, перспективы применения и влияние на тематику информационной безопасности.
18. Технология «блокчейн». Состояние на настоящее время и перспективы ее использования.

Типовые вопросы, выносимые на тестирование

1. Технология VPN может обеспечивать

Целостность, аутентификацию и конфиденциальность передаваемых сообщений

Устойчивую связь на каналах плохого качества

Помехозащищенность передаваемых сообщений

Все перечисленное выше.

2. Внедрение СКУД и современных «интеллектуальных» систем видеонаблюдения позволяет

Повысить капитализацию и инвестиционную привлекательность предприятия

Построить один из «рубежей» комплексной системы информационной безопасности объекта

Эффективно осваивать бюджет СЭБ предприятия

3. Увеличение отношения «сигнал/шум» обеспечивает

надежность передачи сигнала в канале связи

снижение вероятности перехвата опасных сигналов на границе контролируемой зоны

качество воспроизведения сигнала в системах звукоусиления

4. Какой фрагмент шифртекста при шифровании «по Шеннону» соответствует фрагменту 001011010010101 открытого текста при использовании фрагмента ключа шифрования 101101001011000

001011011010011

100110011001101

101100101010110

Правильный фрагмент отсутствует

5. Для активной защиты от утечки речевого сигнала лучше использовать

«Белый шум» в частотном диапазоне от 150 Гц до 8 кГц

«Розовый шум» в частотном диапазоне от 300 Гц до 3.4 кГц

Гармонические сигналы в частотном диапазоне от 20 Гц до 20 кГц

6. Какое утверждение относительно технологии блокчейн вы считаете наиболее верным, полным и объективным

Технология блокчейн обеспечивает анонимность платежей криптовалютами для использования в «теневой экономике» и иных противоправных целях

Блокчейн позволяет создавать криптовалютные «финансовые пирамиды»

Блокчейн - основанная на децентрализованном шифровании с «открытым ключом» технология с перспективами применения в самых разных сферах

Блокчейн - способ зарабатывания биткоинов для майнеров

7. Условием абсолютной стойкости шифра по Шеннону является

Однократное использование ключа шифрования

Использование в «открытом тексте» только цифр и символов латинского алфавита

Статистическая надежность ключа шифрования

Длина ключа шифрования должна быть больше или равна длине исходного сообщения

8. Какие критерии используются для принятия решений в условиях неопределенности

Фурье и Лагранжа

Вальда, Сэвиджа и Гурвица

Бойля и Мариотта

9. TEMPEST это

Принятый в США руководящий документ по противодействию средствам и методам РЭБ в Вооруженных силах блока НАТО

Действующий в США и ряде стран Западной Европы набор стандартов, определяющих защищенность технических средств и объектов от утечки информации по каналу ПЭМИН

Протокол шифрования данных, используемый в системе управления средствами ПВО США

10. Информационная безопасность крупного корпоративного центра обработки данных (ЦОД) обеспечивается

Резервированием каналов связи

Использованием ИБП и резервного электропитания

Системой защиты от НСД к объекту размещения ЦОД, его отдельным серверам и иным компонентам

Внедрением межсетевых экранов, антивирусной защиты и системы DLP

Криптографической защитой передаваемой по каналам связи информации

Всеми перечисленными методами

11. Как определяется понятие «информация» в 149-ФЗ от 27.07.06

Универсальный товар в период развития цифровой экономики

Сведения, сообщения, данные, независимо от формы их представления

Объективное содержание связи между взаимодействующими материальными объектами, проявляющееся в изменении состояния этих объектов

Любые данные, содержащиеся в электронных и печатных документах, имеющих все необходимые реквизиты

12. Какие каналы утечки речевой конфиденциальной информации принято выделять при ведении переговоров в типовом офисном помещении

Акустический и виброакустический

Визуальный

Акустоэлектрический

Все перечисленные выше

13. Что означает сокращение ФСТЭК

Фонд Содружества Технологических и Электротехнических Комиссий

Федеральная Служба по Техническому и Экспортному Контролю

Федеральная Система Технической и Экономической Координации

14. Понятие «Red Equipment» стандарта TEMPEST соответствует

BTCC

OTCC

Измерительному оборудованию, используемому для оценки защищенности от утечек по каналу ПЭМИН

15. Какие меры противодействия доступу к конфиденциальной информации с использованием СТС могут быть реализованы коммерческим предприятием

Введение особого порядка допуска на территорию и в выделенные помещения

Получение статуса субъекта ОРД и реализация «встречных мер» в отношении конкурентов

Периодическое проведение спецобследований выделенных помещений - собственными силами или с привлечением имеющих лицензии фирм

Подавление СТС техническими средствами в период проведения конфиденциальных мероприятий

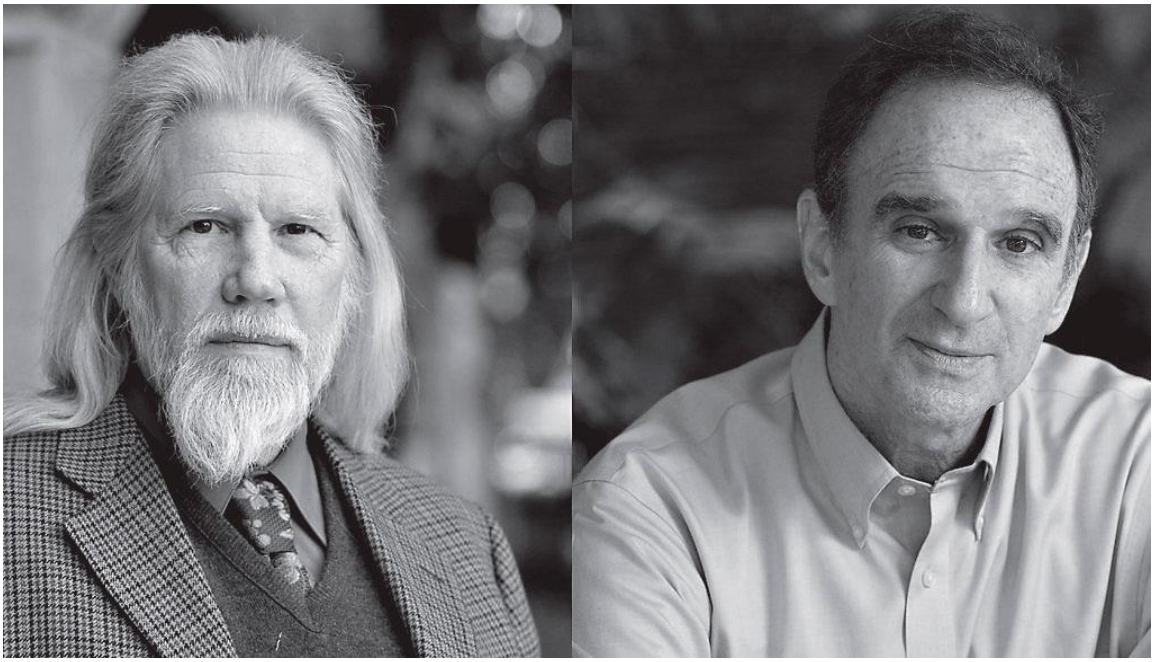
16. Наиболее точные результаты СИ достигаются в условиях

Проведения исследований на объекте, где эксплуатируются технические средства

Специализированной лаборатории с использованием аттестованной безэховой экранированной камеры

Полигона с минимальными индустриальными помехами

17. На фотографиях изображены



У. Диффи и М. Хеллман

Р. Ривест и А. Шамир

Д. Леннон и П. Маккартни

18. Какие органы государственной власти относятся к «Регуляторам» деятельности в области информационной безопасности

Роскомнадзор и Министерство цифрового развития, связи и массовых коммуникаций

ФСТЭК и ФСБ

Совет безопасности Российской Федерации и Администрация Президента Российской Федерации

19. Кто из перечисленных ученых - академиков внес значительный вклад в развитие информационной безопасности в СССР

И.В. Курчатов и А.Д. Сахаров

Н.Г. Басов и А.М. Прохоров

В.А. Котельников и А.Н. Колмогоров

20. К субъектам КИИ относятся

Предприятия ВПК

Системообразующие сетевые предприятия розничной торговли

Предприятия ТЭК и отрасли связи

Предприятия финансового сектора

Крупнейшие строительные компании

21. Какой алгоритм реализует программа PGP

Шифрования с симметричным ключом

Шифрования с «открытым» ключом

Стеганографического преобразования информации

22. На рисунке изображена структурная схема

Обработки почты при конфиденциальном делопроизводстве

Помехозащищенного кодирования

Шифрования с «открытым» ключом

Шифрования по Шеннону

23. Защита информации от утечки по каналу ПЭМИН обеспечивается

Использованием специализированных электронных компонентов и схемотехнических решений

Применением экранирования электромагнитных полей и фильтрацией в цепях распространения сигналов

Зашумлением объекта защиты с использованием сертифицированных генераторов электромагнитных помех

Всеми перечисленными методами

24. Triple DES это

Разработанный и применяемый в США стандарт симметричного шифрования

Модификация DES, обеспечивающая лучшую криптографическую стойкость

Национальный Японский стандарт шифрования с «открытым» ключом

25. Безопасность информации обеспечивается при сохранении ее

Конфиденциальности

Целостности

Доступности

Выполнении всех трех перечисленных выше условий

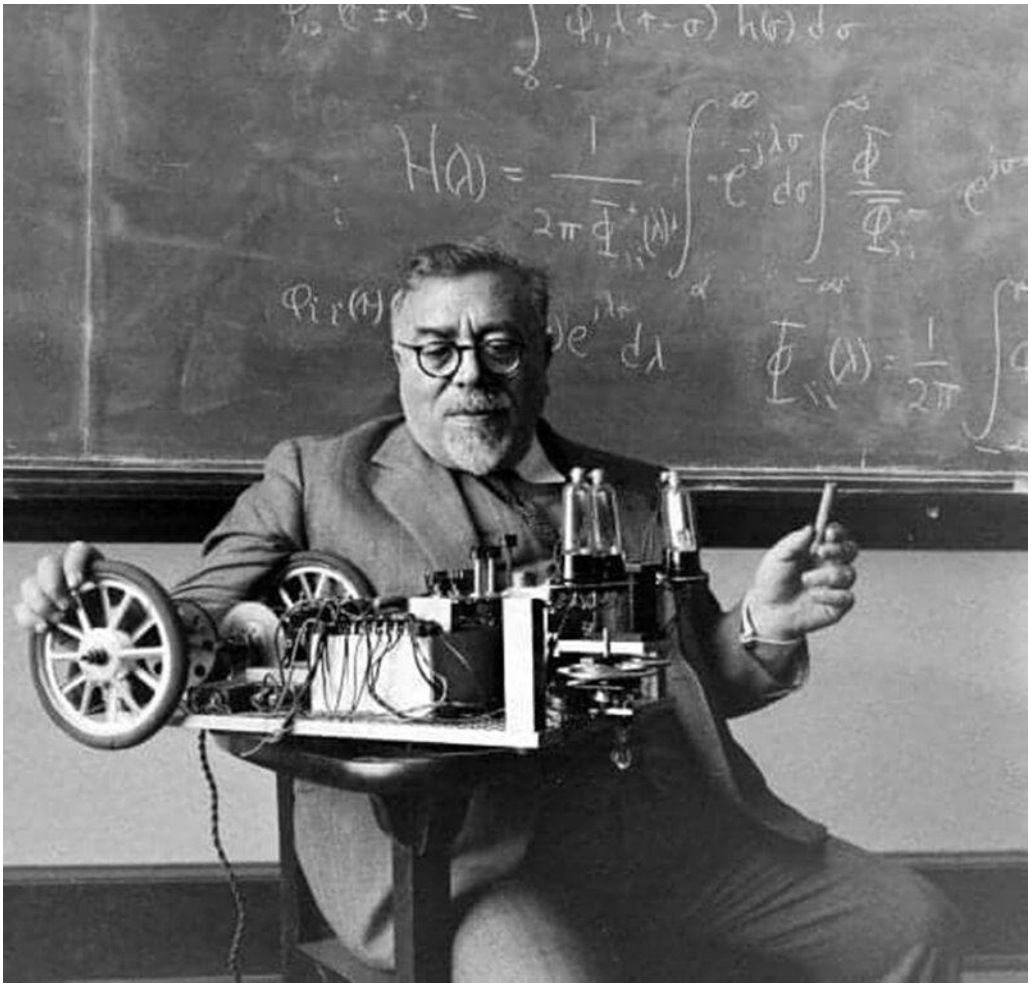
26. Стандартный протокол шифрования А5, применяемый в сетях сотовой подвижной связи GSM-900, обеспечивает защиту передаваемой информации

Во всем тракте передачи информации – от абонентского устройства до абонентского устройства

От базовой станции до Центра коммутации оператора связи

Только в радиоканале от абонентского устройства до работающей с ним базовой станции

27. Выберите из представленных изображений фотографию академика В.А. Котельникова



28. Стеганография это

Разновидность методов блочного шифрования

Метод защиты информации, в котором используется сокрытие самого факта наличия информации

Система помехоустойчивого кодирования с применением векторной графики

29. Пассивная защита от утечки информации по виброакустическому каналу обеспечивается

Применением демпфирующих вставок на трубах систем отопления и водоснабжения и ослабляющих звук экранов перед элементами данных систем

Применением подключаемых к генератору шума вибродатчиков, устанавливаемых на трубах систем отопления и водоснабжения, оконных рамах и стеклах

Специальной конструкцией стеклопакетов и крепления оконных рам в стенах здания

30. Инциденты информационной безопасности, связанные с нарушением доступности, могут вызываться

DDoS атакой на информационную инфраструктуру

Аварийным отключением электропитания оборудования ЦОД

Разрушением или блокированием каналов связи

Деструктивным компьютерным вирусом, заразившим серверное оборудование или ПК и блокирующим их работу

Всеми указанными выше причинами

Типовые задания к проверочным работам

Вариант 1

1. Критерии обеспеченности информационной безопасности. Примеры нарушений по каждому критерию.
2. ПЭМИН как канал утечки информации. Причины возникновения и меры противодействия.

Вариант 2

1. Комплексный подход к вопросам защиты информации. Примеры инцидентов (не менее двух) при отсутствии комплексного системного подхода к защите.
2. Каналы утечки речевой конфиденциальной информации. Типовые меры защиты.

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

Формой контроля знаний по дисциплине «Основы информационной безопасности» являются две текущие аттестации в виде тестов и итоговая аттестация в форме 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 учебного процесса	Тестирование 1,2	УК-2 ПК-4	30 вопросов	Компьютерное тестирование; время, отведенное на процедуру - 45 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%.
Проводится в сроки, устан	Зачет	УК-2 ПК-4	2 вопроса	Зачет проводится в устной форме, путем ответа на	Результаты предоставляются в день проведения зачета	Критерии оценки: «**Зачтено**»: 1. знание лексического и

овленные графиком учебного процесса				вопросы. Время, отведенное на процедуру – 30 минут.		грамматического материала; 2. умение использовать и применять полученные знания на практике; 3. работа на практических занятиях в течение семестра; 4. ответ на вопросы зачета. «**Не зачтено**»: 1. демонстрирует частичные знания по темам дисциплин; 2. незнание лексического и грамматического материала; 3. неумение использовать и применять полученные знания; 4. не работал на практических занятиях; 5. не отвечает на вопросы зачета.

Типовые вопросы к зачету:

1. Понятие Концепции национальной безопасности РФ и место в ней информационной безопасности.
2. Общая характеристика организационных структур разведок развитых зарубежных стран.
3. Сущность Доктрины информационной безопасности РФ. Источники угроз в информационной сфере.
4. Основные задачи обеспечения ИБ РФ (по Доктрине ИБ).
5. Государственная политика обеспечения ИБ РФ (по Доктрине ИБ).
6. Организационная основа системы обеспечения ИБ РФ (по Доктрине ИБ).
7. Основные федеральные законы РФ в области ИБ.
8. Цели, функции и задачи защиты информации.
9. Защита информации и проблема «информационной войны».
10. Понятие о Концепции и стратегиях защиты информации.
11. Критерии отнесения информации к защищаемой.
12. Понятие носителей защищаемой информации, их состав.

13. Определение «государственной тайны» и порядок отнесения к ней сведений.
14. Определение «коммерческой тайны» и порядок отнесения к ней сведений.
15. Понятие «служебной тайны», границы и области ее действия.
16. Организация взаимодействия сторон, связанного с передачей конфиденциальной информации. Понятие о NDA.
17. Понятие «персональные данные», правовые требования по их защите.
18. Понятие критической информационной инфраструктуры (КИИ). Правовые требования по ее защите.
19. Понятие и структура угроз защищаемой информации.
20. Понятие, состав и характеристика источников воздействия на защищаемую информацию.
21. Классификация методов защиты информации и их характеристика.
22. Понятие, назначение и состав кадрового обеспечения защиты информации.
23. Понятие, назначение и состав ресурсного обеспечения защиты информации.
24. Понятие, назначение и состав технологического обеспечения защиты информации.
25. Основные организационные и технологические документы по защите информации.
26. Контрольные мероприятия по защите информации. Их виды и характеристики.
27. Роль науки в деятельности, связанной с информационной безопасностью.
28. Конфиденциальность, доступность и целостность как критерии информационной безопасности.
29. Инциденты информационной безопасности, связанные с нарушением доступности и целостности. Примеры.
30. Требование комплексности при защите информации.
31. Понятия «модели угроз» и «модели нарушителя» в информационной безопасности.
32. Основные факторы и причины утечки информации.
33. Правовые и организационные методы защиты информации.
34. Основные технические каналы утечки информации.
35. Криптографическая защита информации. Основные понятия.
36. Стеганографические методы защиты информации.
37. Математические основы криптографии и криптоанализа.
38. «Классическая» криптография Шеннона.
39. Криптография с открытым ключом.
40. Физические основы информационной безопасности. Отношение сигнал/шум
41. Программа и стандарты TEMPEST, основные подходы.
42. Понятие «специальные исследования».
43. Понятие «специальные проверки».
44. Понятие «специальные обследования».
45. Понятие «основные технические средства и системы».
46. Понятие «вспомогательные технические средства и системы».
47. Основные этапы аттестации объектов информатизации на соответствие требованиям безопасности.
48. Методы защиты от утечки информации по каналу ПЭМИН.

49. Методы защиты речевой информации от утечки по акустическому и виброакустическому каналам.
50. Комплаенс в информационной безопасности.
51. Кибербезопасность как составляющая информационной безопасности.
52. Основные элементы комплексной информационной безопасности распределенной корпоративной ИТ - системы.

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

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ
КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ «ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Направление подготовки: 01.03.02 Прикладная математика и информатика

Профиль: Программирование, математическое моделирование

Уровень высшего образования: бакалавриат

Форма обучения: очная

Королев
2023

1. Общие положения

Цель дисциплины:

– формирование у студентов специализированной базы знаний по фундаментальным проблемам информационной безопасности в условиях становления современного информационного общества, в использовании организационно-технических механизмов обеспечения защиты информационных объектов;

– выработать и закрепить у обучающихся базовые умения и навыки в применении технологий обеспечения информационной безопасности для защищаемых объектов.

Задачи дисциплины:

– ознакомление студентов с методологическими подходами применения и эксплуатации основных технических средств информационной безопасности защищаемых объектов;

– изучение основных методов определения параметров, характеристик и условий применения технических средств защиты на основе анализа возможных угроз информационной безопасности и потенциальных каналов утечки информации;

– формирование у студентов способности самостоятельно решать поставленные задачи в области информационной безопасности с помощью существующих принципов, методов и технологий в различных организационных структурах, по базовым направлениям и применительно к типовым информационным объектам.

2. Указания по проведению практических занятий

Практическое занятие 1.

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

Образовательные технологии: *компьютерные технологии обучения*

Тема и содержание практического занятия: *Тема 1. Концепция информационной безопасности.*

Цель работы: Получить знания и практические навыки по применению концептуальной модели информационной безопасности, её основным характеристикам и особенностям построения.

Основные положения темы занятия:

1. Определения и виды обеспечения системы информационной безопасности и основные требования к ней.

2. Характеристика действий, приводящих к неправомерному овладению конфиденциальной информацией.

Вопросы для обсуждения:

1. Определение и характеристика угроз конфиденциальной информации.

2. Порядок классификации угроз конфиденциальной информации по различным признакам.

3. Классификация и особенности действий, приводящих к неправомерному овладению конфиденциальной информацией.

4. Характеристика форм и методов недобросовестной конкуренции в современном мире.

Продолжительность занятия – 4 ч.

Практическое занятие 2.

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

Образовательные технологии: *компьютерные технологии обучения*

Тема и содержание практического занятия: *Тема 2. Основные направления обеспечения информационной безопасности.*

Цель работы: Получить знания и практические навыки по основным направлениям информационной безопасности, как нормативно-правовым категориям, определяющим комплексные меры защиты информационных объектов на государственном уровне, а также на уровне предприятия, организации и отдельной личности.

Основные положения темы занятия:

1. Основные определения, состав и особенности реализации правовой и организационной защиты информационных объектов.

2. Предназначение, состав и особенности построения службы безопасности предприятия, фирмы, реализация инженерно-технической защиты информационных объектов.

Вопросы для обсуждения:

1. Состав, классификация и особенности применения физических средств защиты информационных объектов.

2. Основные задачи, состав, классификация и особенности применения аппаратных средств защиты персональных компьютеров и сетей.

3. Предназначение, состав, классификация и особенности применения программных средств защиты информации от чужого вторжения.

4. Особенности применения криптографических средств защиты информации в мире коммерческой деятельности.

Продолжительность занятия – 4 ч.

Практическое занятие 3.

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

Образовательные технологии: *компьютерные технологии обучения*

Тема и содержание практического занятия: *Тема 3. Основные способы защиты информации.*

Цель работы: Получить знания и практические навыки по отдельным способам защиты информации, а также по составу и особенностям применения основных организационных и технических мероприятий по защите информационных объектов.

Основные положения темы занятия:

1. Характеристика каналов распространения информации и порядок реализации защитных действий от неправомерного овладения конфиденциальной информацией.

2. Взаимосвязь источников информации, целей защиты и механизмов защиты в процессе телекоммуникационного обмена сведениями.

Вопросы для обсуждения:

1. Анализ основных факторов и обстоятельств, приводящих к разглашению конфиденциальной информации.

2. Характеристика основных способов пресечения разглашения конфиденциальной информации.

3. Состав и классификация основных каналов распространения сведений, как средств обмена деловой и научной информацией.

4. Главные направления воспитательно- профилактической деятельности, как средств воздействия на чувства, волю и характер сотрудников в интересах формирования у них способности хранить тайну и соблюдать правила работы с закрытой информацией.

Продолжительность занятия – 4 ч.

Практическое занятие 4.

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

Образовательные технологии: *компьютерные технологии обучения*

Тема и содержание практического занятия: *Тема 4. Защита информации от утечки по техническим каналам связи.*

Цель работы: Получить знания и практические навыки по применению защитных мер от утечки информации по техническим каналам связи

Основные положения темы занятия:

1. Структура канала утечки информации, классификация технических каналов и особенности их проявления.

2. Краткий обзор визуально-оптических, акустических и электромагнитных каналов утечки информации, особенности защиты информации по ним.

Вопросы для обсуждения:

1. Защита информации от утечки по цепям электропитания и заземления.

2. Защита информации от утечки за счёт взаимного влияния проводов и линий связи, в том числе в волоконно-оптических линиях связи.

3. Защита информации от утечки за счёт электромагнитного навязывания сигнала.

4. Защита информации от утечки по материально-вещественным каналам распространения информации.

Продолжительность занятия – 4 ч.

Практическое занятие 5.

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

Образовательные технологии: *компьютерные технологии обучения*

Тема и содержание практического занятия: *Тема 5. Способы противодействия несанкционированному доступу к источникам конфиденциальной информации.*

Цель работы: Получить знания и практические навыки по основным способам противодействия несанкционированному доступу к источникам конфиденциальной информации.

Основные положения темы занятия:

1. Характеристика обобщённой модели способов несанкционированного доступа к источникам конфиденциальной информации и их взаимосвязь друг с другом.

2. Обзор технических средств несанкционированного доступа к информации и их основные возможности.

Вопросы для обсуждения:

1. Особенности защиты от наблюдения, съёмки и фотографирования, как способа ведения разведки с целью получения информации об объектах.

2. Особенности защиты от подслушивания переговоров, как способа ведения разведки и промышленного шпионажа.

3. Особенности формирования, состав и порядок применения частной модели фотографического контакта.

4. Методика организации противодействия подслушиванию переговоров посредством микрофонных систем.

Продолжительность занятия – 4 ч.

Практическое занятие 6.

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

Образовательные технологии: *компьютерные технологии обучения*

Тема и содержание практического занятия: *Тема 6. Особенности защиты информационных объектов с помощью технических средств.*

Цель работы: Получить знания и практические навыки по методике защиты информационных объектов с помощью современных технических средств.

Основные положения темы занятия:

1. Предназначение, классификация и особенности применения акустических систем радиоподслушивания (радиозакладок), их параметры и основные характеристики.

2. Характеристика и классификация основных средств обнаружения радиосигналов, понятие радиоэлектронных помех, их разновидности и порядок постановки.

Вопросы для обсуждения:

1. Порядок организации противодействия контактному подключению к линиям связи, основные средства противодействия.

2. Порядок организации противодействия бесконтактному подключению к линиям связи, основные средства противодействия.

3. Организация защиты информации от радиоперехвата, обзор характеристик средств противодействия.

4. Состав, порядок построения и использования частной и параметрической моделей радиоперехвата.

Продолжительность занятия – 4 ч.

Практическое занятие 7.

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

Образовательные технологии: *компьютерные технологии обучения*

Тема и содержание практического занятия: *Тема 7. Защитные меры при работе с зарубежными партнёрами.*

Цель работы: Получить знания и практические навыки по организации работы с зарубежными партнёрами с использованием защитных мероприятий и способов сохранения конфиденциальной информации, защиты коммерческой тайны и интеллектуальной собственности предприятия, фирмы, организации.

Основные положения темы занятия:

1. Характеристика основных направлений взаимодействия с зарубежными партнёрами и порядок организации научно-технического сотрудничества с ними.

2. Особенности технологического обмена результатами совместной деятельности и порядок его регулирования, анализ возможных условий разглашения сведений, составляющих коммерческую тайну в международных сделках.

Вопросы для обсуждения:

1. Основные формы и особенности защиты конфиденциальной информации при работе с зарубежными партнёрами по заключённым договорам и соглашениям.

2. Особенности подготовки и документального обеспечения визитов зарубежных организаций, основные режимные меры их сопровождения и взаимодействия с ними.

3. Порядок приёма зарубежных партнёров, организация деловых встреч и переговоров.

4. Порядок представления итоговых документов по результатам деловых встреч и совместной деятельности с зарубежными партнёрами, ответственность структурных подразделений и должностных лиц за сохранение конфиденциальной информации и других производственных секретов.

Продолжительность занятия – 4 ч.

Практическое занятие 8.

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

Образовательные технологии: *компьютерные технологии обучения*

Тема и содержание практического занятия: *Тема 8. Методика разработки системы защиты информации на предприятии.*

Цель работы: Получить знания и практические навыки по основным этапам методики разработки или совершенствования системы защиты информации на предприятии.

Основные положения темы занятия:

1. Порядок разработки системы защиты информации на предприятии, характеристика основных стадий разработки и этапов работы.

2. Общий порядок действий по обеспечению информационной безопасности на основных этапах разработки системы защиты, методика проведения аудита выделенных помещений и её особенности.

Вопросы для обсуждения:

1. Методика оценки эффективности системы защиты информации на предприятии в соответствии с принципом комплексного подхода.

2. Понятия критериев и показателей эффективности системы защиты информации, их основные различия и порядок применения.

3. Определение важности защищаемых объектов на основании результатов оценки эффективности и грифов обрабатываемой информации на них.

4. Основные методы, способы и мероприятия по достижению конечных целей информационной безопасности предприятия на различных этапах её построения и эксплуатации.

Продолжительность занятия – 4 ч.

3. Указания по проведению лабораторного практикума

Не предусмотрено учебным планом.

4. Указания по проведению самостоятельной работы студентов

Цель самостоятельной работы: подготовить студентов к самостоятельному научному творчеству.

Задачи самостоятельной работы:

1) расширить представление в области информационной безопасности и существующих средств защиты информации;

2) привить навыки самостоятельного решения нестандартных задач в области применения защитных средств и технологий.

Тематическое содержание самостоятельной работы представлено в таблице:

№ п/п	Виды самостоятельной работы	Количество часов	Перечень заданий
1.	Вопросы, выносимые на самостоятельное изучение	15	1. Особенности шифрования данных псевдослучайными числами. 2. Основные методы шифрования информации и их характеристика. 3. Порядок применения поточных и блочных шифров, понятие криптографического протокола. 4. Криптографические системы с открытым ключом и их особенности применения. 5. Методы использования специальных свойств компьютерных форматов. 6. Подходы к использованию электронной цифровой подписи и методы хеширования сообщений. 7. Методы использования избыточности аудио- и видеоинформации в компьютерной стеганографии. 8. Характеристика современных распространённых методов биометрической идентификации личности и особенности их применения. 9. Реализация технологии речевой подписи (аудиомаркирования) сообщений с применением компьютерных технологий. 10. Практическое применение защитной технологии «речевая подпись» в современном мире.

2.	Тематика докладов	15	1. Активные способы противодействия прослушиванию помещений по абонентским линиям связи. 2. Характеристика основных способов защиты абонентских телефонных линий связи от бесконтактного съёма информации. 3. Характеристика способов съёма акустической информации со стен и потолочных перекрытий охраняемых муниципальных объектов. 4. Характеристика способов съёма акустической информации с металлических труб и оконных стёкол охраняемых муниципальных объектов. 5. Характеристика способов съёма акустической информации в помещении по линии электросети охраняемых муниципальных объектов. 6. Характеристика пассивных способов противодействия прослушивания охраняемых помещений по абонентской линии связи. 7. Методика применения телефонолокационного способа съёма акустических сигналов в муниципальных защищаемых помещениях. 8. Характеристика основных устройств противодействия съёму информации в муниципальных защищаемых помещениях. 9. Основные компоненты охранной сигнализации при использовании различных датчиков. 10. Характеристика современных телевизионных средств охранной сигнализации. 11. Характеристика сетевых пассивных помехоподавляющих фильтров низких и высоких частот. 12. Методика обнаружения сигналов линейных сетевых закладок и особенности её применения. 13. Методика обнаружения оптических сигналов передатчиков ИК диапазона и особенности её применения. 14. Методика обнаружения активных прослушивающих устройств с помощью индикатора электромагнитного поля. 15. Доктрина ИБ РФ: критически важные информационные объекты. 16. Доктрина ИБ РФ: направления обеспечения информационной безопасности. 17. Классификация защищаемого информационного ресурса. 18. Конфиденциальная информация и ее характеристика. 19. Секретная информация как объект информационной безопасности. 20. Организационное обеспечение информационной безопасности. 21. Техническое обеспечение информационной безопасности. 22. Правовое обеспечение информационной безопасности. 23. Организационная система обеспечения ИБ РФ. 24. Персональные данные как объект ИБ. 25. Понятие о теории защиты информации.
3.	Выполнение практических заданий	15	1. Основные криптографические методы защиты электронной документации и данных. 2. Современные технологии обеспечения безопасности на основе индивидуальных особенностей человека.
4	Подготовка к зачету	15	Проработка лекций, практик, изучение рекомендованной литературы. Консультации у преподавателя.

5. Указания по проведению контрольных работ (подготовке рефератов) для обучающихся очной формы обучения

Основной целью контрольной работы (реферата) является закрепление основных положений дисциплины. Контрольная работа (реферат) может включать в себя рассмотрение теоретических вопросов дисциплины, а также их практическое приложение.

5.1 Требования к структуре

Структура контрольной работы (реферата) 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 (для теоретических вопросов) и методы решения задачи (для практических заданий).
2. При определении целей и задач 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, сформулированных во введении, и заканчивается констатацией итогов (для теоретических вопросов) и решение задачи в MSExcel с описанием основных этапов.
4. Приветствуется иллюстрация содержания работы таблицами, графическим материалом (рисунками, схемами, скриншотами и т.п.).
5. Необходимо давать ссылки на используемую Вами литературу.
6. Заключение должно содержать сделанные автором работы выводы, итоги исследования и результаты решения задачи.
7. Вслед за заключением идет список литературы, который должен быть составлен в соответствии с установленными требованиями. Если в работе имеются положения, они оформляются на отдельных листах, и должны быть соответственно пронумерованы.

5.3 Требования к оформлению

Объём контрольной работы (реферата) – 12-17 печатных страниц формата А4, напечатанного с одной стороны текста. Титульный лист – принятый в «МГОТУ» для оформления подобных видов работ. Оформляется в MS Word или другом текстовом редакторе по следующим правилам:

1. Шрифт TimesNewRoman, кегль 12-14, интервал между строками 1,5 строки, поля: верхнее и нижнее по 2 см, левое – 3 см, правое – 1 см. Отступ первой строки – 1,25см.
2. Все заголовки оформляются стилями заголовков. При этом необходимо изменить шрифт на TimesNewRoman, кегль до 16 (в зависимости от уровня заголовка), цвет черный.
3. Содержание (оглавление) оформляется по всем требованиям текстового процессора
4. Обязательное наличие списка используемых источников. При этом в тексте указать в квадратных скобках номер используемого источника (литературы).

6. Перечень основной и дополнительной учебной литературы

Основная литература:

1. Информационная безопасность предприятия: Учебное пособие / Н.В. Гришина. - 2-е изд., доп. - М.: Форум: НИЦ ИНФРА-М, 2015. - 240 с.: ил.; 60x90 1/16. - (Высшее образование: Бакалавриат). (обложка) ISBN 978-5-00091-007-8http://znanium.com/bookread2.php?book=491597

2. Загинайлов Ю.Н. Основы информационной безопасности: курс визуальных лекций : учебное пособие / Ю.Н. Загинайлов. - М. ; Берлин : Директ-Медиа, 2015. - 105 с. : ил. - Библиогр. в кн. - ISBN 978-5-4475-3947-4 ; То же [Электронный ресурс]. - URL://biblioclub.ru/index.php?page=book&id=362895

3. Информационная безопасность: учебное пособие под общ. редакцией проф. Ясенева В.Н.; Министерство образования и науки Российской Федерации, Национальный исследовательский Нижегородский государственный университет им. Н.И. Лобачевского - Нижний Новгород, 2017. - 198 с. : УДК 311(075.8) ББК У051; [Электронный ресурс]:
http://www.iee.unn.ru/wp-content/uploads/sites/9/2014/09/Uchebnoe-posobie-po-IB-pod-redaktsiej-YAseneva-V.N.-2017.pdf

4. 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:

1. Е.В. Вострецова Основы информационной безопасности; Учебное пособие; Министерство образования и науки Российской Федерации, Уральский федеральный университет, Екатеринбург, Издательство Уральского университета 2019; 204 с., ISBN 978-5-7996-2677-8, https://elar.urfu.ru/bitstream/10995/73899/3/978-5-7996-2677-8_2019.pdf

2. Безопасность объектов критической информационной инфраструктуры организации. Общие рекомендации (версия 1.0); АРСИБ, Москва 2019, http://aciso.ru/news/3948/

3. А. Першин, Безопасность мобильных технологий в корпоративном секторе. Общие рекомендации (версия 2.0); АРСИБ, Москва 2016, http://aciso.ru/news/3901/

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

Интернет-ресурсы:
http://www.znanium.com/ - электронно-библиотечная система
http://www.e.lanbook.com/ - ЭБС Издательства "ЛАНЬ"
http://www.rucont.ru/- электронно-библиотечная система
http://www.biblioclub.ru/ -университетская библиотека онлайн

8. Перечень информационных технологий

Перечень программного обеспечения: *MSOffice.*
Информационные справочные системы:

1. Ресурсы информационно-образовательной среды Технологического университета
2. Информационно – справочные (правовые) системы: «Консультант +».