Аннотация к рабочей программе дисциплины «Основы информационной безопасности»

Цель преподавания дисциплины

Ознакомление студентов с основами теории безопасности информационных систем, правовым регулирование в области защиты информации, принципами организации аппаратно-программных способов защиты информации в организациях и предприятиях различных направлений деятельности и различных форм собственности для использования полученных знаний в дальнейшем образовательном процессе на старших курсах.

Задачи изучения дисциплины:

- ознакомить студентов с основами теории безопасности информационных систем;
- ознакомить студентов с основами правового регулирования в области защиты информации;
- обучить принципам организации аппаратно-программных способов защиты информации;
- научить студентов универсальным методам защиты информации и условиями их применения.

Компетенции, формируемые в результате освоения дисциплины

ПК-2 – Способен проектироват**ь** биотехнически**е** систем**ы** и технологи**и**

ПК-2.3 – Проектирует детал**и** и узл**ы** биотехнических систем медицинского, экологического и биометрического назначения в соответствии с техническим заданием с использованием средств автоматизации проектирования

ПК-2.5 - Контролирует оформление и соответстви**е** законченных проектно-конструкторских работ, проектов и технической документации на изделия и устройства медицинского и экологического назначения нормативным документам

Разделы дисциплины:

Введение в информационную безопасность. Понятие защищенности в автоматизированных системах. Основы законодательства РФ в области информационной безопасности и защиты информации. Конфиденциальная информация и ее защита. Лицензирование и сертификация в области обеспечения безопасности информации. Технические средства обеспечения информационной безопасности. Криптографические методы защиты информации. Каналы утечки информации. Угроза безопасности информации АСОД и субъектов информационных отношений.

МИНОБРНАУКИ РОССИИ
Юго-Западный государственный университет

УТВЕРЖДАЮ:
И.о. декана факультета
фундаментальной и прикладной информатики
(наименование ф-та полностью)

М.О. Таныгин
(подпись, инициалы, фамилия)

«31» 08 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Основы информационной безопасности
(наименование дисциплины)

ОПОП ВО 12.03.04 Биотехнические системы и технологии
шифр и наименование направление подготовки (специальности)

Биотехнические и медицинские аппараты и системы
наименование направленности (профиля, специализации)

форма обучения *очная*
очная, очно-заочная, заочная

Курск – 2021

Рабочая программа дисциплины «Основы информационной безопасности» составлена в соответствии с ФГОС ВО – бакалавриат по направлению подготовки (специальности) 12.03.04 Биотехнические системы и технологии на основании учебного плана ОПОП ВО 12.03.04 Биотехнические системы и технологии, направленность «Биотехнические и медицинские аппараты и системы», одобренного Ученым советом университета (протокол № 9 «25» июня 2021 г.).

Рабочая программа дисциплины обсуждена и рекомендована к реализации в образовательном процессе для обучения студентов по ОПОП ВО 12.03.04 Биотехнические системы и технологии на основании учебного плана ОПОП ВО 12.03.04 Биотехнические системы и технологии, направленность «Биотехнические и медицинские аппараты и системы» на заседании кафедры информационной безопасности № 11 «28» июня 2021 г.

Зав. кафедрой _____Таныгин М.О.

Разработчик программы
к.т.н., доцент_____ Ефремов М.А.
(ученая степень и ученое звание, Ф.И.О.)

Согласовано: на заседании кафедры биомедицинской инженерии протокол № 1«31» августа 2021 г.

Зав. кафедрой _____Кореневский Н.А.

Директор научной библиотеки _____ Макаровская В.Г.

Рабочая программа дисциплины «Основы информационной безопасности» пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 12.03.04 Биотехнические системы и технологии, направленность «Биотехнические и медицинские аппараты и системы», одобренного Ученым советом университета протокол №___«__»_____20___г., на заседании кафедры_____ .
(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

Рабочая программа дисциплины «Основы информационной безопасности» пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 12.03.04 Биотехнические системы и технологии, направленность «Биотехнические и медицинские аппараты и системы», одобренного Ученым советом университета протокол №___«__»_____20___г., на заседании кафедры_____ .
(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

Рабочая программа дисциплины «Основы информационной безопасности» составлена в соответствии с ФГОС ВО – бакалавриат по направлению подготовки (специальности) 12.03.04 Биотехнические системы и технологии на основании учебного плана ОПОП ВО 12.03.04 Биотехнические системы и технологии, направленность «Биотехнические и медицинские аппараты и системы», одобренного Ученым советом университета (протокол № 9 «25» 06 2021 г.).

Рабочая программа дисциплины обсуждена и рекомендована к реализации в образовательном процессе для обучения студентов по ОПОП ВО 12.03.04 Биотехнические системы и технологии на основании учебного плана 12.03.04 Биотехнические системы и технологии, направленность «Биотехнические и медицинские аппараты и системы» на заседании кафедры информационной безопасности №1 «30» 08 2021 г.

Зав. кафедрой _____ Таныгин М.О.

Разработчик программы
к.т.н., доцент _____ Ефремов М.А.
(ученая степень и ученое звание, Ф.И.О.)

Согласовано: на заседании кафедры биомедицинской инженерии протокол № 1 «31» 08 2021 г.

Зав. кафедрой _____ Кореневский Н.А.

Директор научной библиотеки _____ Макаровская В.Г.

Рабочая программа дисциплины «Основы информационной безопасности» пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 12.03.04 Биотехнические системы и технологии, направленность «Биотехнические и медицинские аппараты и системы», одобренного Ученым советом университета протокол №7 «25» 02 2020 г., на заседании кафедры информационной безопасности протокол №11 от 30.06.2022 г.
(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

Рабочая программа дисциплины «Основы информационной безопасности» пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 12.03.04 Биотехнические системы и технологии, направленность «Биотехнические и медицинские аппараты и системы», одобренного Ученым советом университета протокол № 9 «25» 06 2021 г., на заседании кафедры информационной безопасности протокол №1 от 30.08.2023 г.
(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

1. Цель и задачи дисциплины. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы

1.1. Цель преподавания дисциплины

Ознакомление студентов с основами теории безопасности информационных систем, правовым регулированием в области защиты информации, принципами организации аппаратно-программных способов защиты информации в организациях и предприятиях различных направлений деятельности и различных форм собственности для использования полученных знаний в дальнейшем образовательном процессе на старших курсах.

1.2. Задачи изучения дисциплины

- ознакомить студентов с основами теории безопасности информационных систем;
- ознакомить студентов с основами правового регулирования в области защиты информации;
- обучить принципам организации аппаратно-программных способов защиты информации;
- научить студентов универсальным методами защиты информации и условиями их применения.

1.3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы

Таблица 1.3 – Результаты обучения по дисциплине

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
ПК-2	Способен проектировать биотехнические системы и	ПК-2.3 Проектирует детали и узлы биотехнических	***Знать:*** современные методы и средства контроля состояния технической защиты информации на

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
	технологии	систем медицинского, экологического и биометрического назначения в соответствии с техническим заданием с использованием средств автоматизации проектирования	объектах автоматизации ***Уметь:*** планировать перечень работ по контролю состояния технической защиты информации на объектах автоматизации ***Владеть (****или* ***Иметь опыт деятельности):*** понятийно-терминологическим аппаратом в области информационной безопасности
		ПК-2.5 Контролирует оформление и соответствие законченных проектно-конструкторских работ, проектов и технической документации на изделия и устройства медицинского и экологического назначения нормативным документам	***Знать:*** нормативную базу, методы и организацию работ по технической защите информации ***Уметь:*** применять на практике современные средства контроля состояния технической защиты информации ***Владеть (****или* ***Иметь опыт деятельности):*** способами и технологиями защиты автоматизированных систем от воздействий злоумышленников

2. Указание места дисциплины в структуре основной профессиональной образовательной программы

Дисциплина «Основы информационной безопасности» входит в часть, формируемую участниками образовательных отношений блока 1 «Дисциплины (модули»») основной профессиональной образовательной программы – программы бакалавриата 12.03.04 Биотехнические системы и технологии, профиль «Биотехнические и медицинские аппараты и системы». Дисциплина изучается на 3 курсе в 5 семестре.

3. Объем дисциплины в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоёмкость (объём) дисциплины составляет 5 зачётных единиц, 72 часа

Таблица 3 – Объем дисциплины

Виды учебной работы	Всего, часов
Общая трудоемкость дисциплины	72
Контактная работа обучающихся с преподавателем по видам учебных занятий (всего)	36
в том числе:	
лекции	18
лабораторные занятия	0
практические занятия	18
Самостоятельная работа обучающихся (всего)	35.9
Контроль (подготовка к зачету)	0
Контактная работа по промежуточной аттестации (всего АттКР)	0.1
в том числе:	
зачет	0.1
зачет с оценкой	не предусмотрен
курсовая работа (проект)	не предусмотрена
экзамен (включая консультацию перед экзаменом)	не предусмотрена

4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1. Содержание дисциплины

Таблица 4.1.1 – Содержание дисциплины, структурированное по темам (разделам)

№ п/п	Раздел (тема) дисциплины	Содержание
1.	Введение в информационную безопасность	Информационная сфера (среда). Целостность Доступность. Конфиденциальность. Основные принципы обеспечения информационной безопасности. Системность подхода. Комплексность подхода. Принцип разумной достаточности.
2.	Понятие защищенности в автоматизированных системах	Понятие защищенности. Меры и средства защиты информации. Способы обеспечения информационной безопасности.
3.	Основы законодательства РФ в области информационной безопасности и защиты информации	Федеральный закон «Об информации, информационных технологиях и о защите информации». Государственная тайна. Система обозначения сведений: «Особой важности», «Совершенно секретно», «Секретно».
4.	Конфиденциальная информация и ее защита	Коммерческая тайна. Служебная тайна. Профессиональная тайна. Персональные данные.
5.	Лицензирование и сертификация в области обеспечения безопасности информации	Лицензирование. Организационное обеспечение информационной безопасности. Организационные (административные) средства защиты.
6.	Технические средства обеспечения информационной безопасности	Основные технические средства. Вспомогательные технические средства и системы обеспечения информационной безопасности.
7.	Криптографические методы защиты информации	Базовые определения и принципы криптографии. Симметричные криптосистемы. Блочные шифры. Сеть Фейстеля. Поточные шифры. Регистры сдвига с обратной связью. Асимметричные криптосистемы. Криптосистема RSA.
8.	Каналы утечки информации	Каналы утечки информации. Побочные электромагнитные излучения ТСПИ. Побочные электромагнитные излучения на частотах работы высокочастотных генераторов ТСПИ. Причинами возникновения электрических каналов утечки информации. Способы и средства подавления электронных устройств перехвата речевой информации
9.	Угроза безопасности информации АСОД и субъектов информационных отношений	Угроза интересов субъекта информационных отношений. Классификация угроз безопасности. Классификация каналов проникновения в систему и утечки информации. При контактном НСД. При бесконтактном НСД. Неформальная модель нарушителя в АСОД

Таблица 4.1.2 – Содержание дисциплины и её методическое обеспечение

№	Раздел (тема) дисциплины	Виды деятельности	Учебно-методич	Формы текущего	Компетенции

п/п		лек., час	№ лб.	№ пр.	еские материалы	контроля успеваемости *(по неделям семестра)*	
1.	Введение в информационную безопасность	2		1	О-1,2 Д-1-4,6 МУ-1	С, Т 2	ПК-2.3
2.	Понятие защищенности в автоматизированных системах	2		2	О-1,2 Д-4,6,8 МУ-2	С, Т 4	ПК-2.3
3.	Основы законодательства РФ в области информационной безопасности и защиты информации	2			О-1,2 Д-6-8	С 6	ПК-2.3
4.	Конфиденциальная информация и ее защита	2			О-1,2 Д-4,6-8	С 8	ПК-2.3
5.	Лицензирование и сертификация в области обеспечения безопасности информации	2			О-1,2 Д-4,6,8	С 10	ПК-2.3 ПК-2.5
6.	Технические средства обеспечения информационной безопасности	2		3	О-2 Д-4-8 МУ-3	С, Т 12	ПК-2.3 ПК-2.5
7.	Криптографические методы защиты информации	2		4	О-1,2 Д-4,6,8 МУ-4	С, Т 14	ПК-2.5
8.	Каналы утечки информации	2		5	О-1,2 Д-2,4,6 МУ-5	С, Т 16	ПК-2.3
9.	Угроза безопасности информации АСОД и субъектов информационных отношений	2		6	О-1,2 Д-3-8 МУ-6	С, Т 18	ПК-2.3 ПК-2.5

С – собеседование, Т – тест, Кейс-задача

4.2. Лабораторные работы и практические занятия

4.2.1. Практические занятия

Таблица 4.2.1 – Практические занятия

№	Наименование лабораторной работы	Объем, час.
1.	Шифрование методом простой замены	2
2.	Шифрование методом полиалфавитной замены	2
3.	Шифрование методом перестановок (маршруты Гамильтона)	2
4.	Схема Шамира разделения секрета	4
5.	Шифрование аналитическими методами (методами матричной алгебры)	4

6.	Системы с открытым ключом. Алгоритм RSA.	4
Итого		18

4.3. Самостоятельная работа студентов (СРС)

Таблица 4.5 – Самостоятельная работа студентов

№	Наименование раздела учебной дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час.
1.	Введение в информационную безопасность	2 неделя	4
2.	Понятие защищенности в автоматизированных системах	4 неделя	4
3.	Основы законодательства РФ в области информационной безопасности и защиты информации	6 неделя	4
4.	Конфиденциальная информация и ее защита	8 неделя	4
5.	Лицензирование и сертификация в области обеспечения безопасности информации	10 неделя	4
6.	Технические средства обеспечения информационной безопасности	12 неделя	4
7.	Криптографические методы защиты информации	14 неделя	4
8.	Каналы утечки информации	16 неделя	4
9.	Угроза безопасности информации АСОД и субъектов информационных отношений	18 неделя	4
Итого			36

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

Студенты могут при самостоятельном изучении отдельных тем и вопросов дисциплин пользоваться учебно-наглядными пособиями, учебным оборудованием и методическими разработками кафедры в рабочее время, установленное Правилами внутреннего распорядка работников.

Учебно-методическое обеспечение для самостоятельной работы обучающихся по данной дисциплине организуется:

библиотекой университета:

- библиотечный фонд укомплектован учебной, методической, научной, периодической, справочной и художественной литературой в соответствии с УП и данной РПД;
- имеется доступ к основным информационным образовательным ресурсам, информационной базе данных, в том числе библиографической, возможность выхода в Интернет.

кафедрой:

- путем обеспечения доступности всего необходимого учебно-методического и справочного материала;
- путем предоставления сведений о наличии учебно-методической литературы, современных программных средств.

путем разработки:

- методических рекомендаций, пособий по организации самостоятельной работы аспирантов;
- заданий для самостоятельной работы;
- вопросов к зачету;
- методических указаний к выполнению практических работ и т.д.

типографией университета:

- помощь авторам в подготовке и издании научной, учебной и методической литературы;
- удовлетворение потребности в тиражировании научной, учебной и методической литературы.

6. Образовательные технологии. Технологии использования воспитательного потенциала дисциплины

Образовательные технологии.

Реализация компетентностного подхода предусматривает широкое использование в образовательном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования общепрофессиональных компетенций обучающихся. В рамках дисциплины предусмотрены выполнение в ходе практически работ и практикоориентированных заданий.

Таблица 6.1 – Интерактивные образовательные технологии, используемые при проведении аудиторных занятий

№	Наименование раздела (темы лекции, практического или лабораторного занятия)	Используемые интерактивные образовательные технологии	Объём, час.
1.	Выполнение практической работы «Шифрование методом простой замены»	Выполнение студентами интерактивных заданий по реализации шифрования методом простой замены	2
2.	Лекция «Конфиденциальная информация и ее защита»	Разбор конкретных ситуаций по классификации конфиденциальной информации и способах ее защиты	2
3.	Выполнение практической работы «Шифрование методом перестановок»	Выполнение студентом интерактивных заданий по реализации шифрования методом перестановок	2
4.	Лекция «Криптографические методы защиты информации»	Разбор конкретных ситуаций по применимости криптографических методов защиты информации в зависимости от типа	2

		информационных систем	
Итого			8

Технологии использования воспитательного потенциала дисциплины

Содержание дисциплины обладает значительным воспитательным потенциалом, поскольку в нем аккумулирован научный опыт человечества. Реализация воспитательного потенциала дисциплины осуществляется в рамках единого образовательного и воспитательного процесса и способствует непрерывному развитию личности каждого обучающегося. Дисциплина вносит значимый вклад в формирование общей и профессиональной культуры обучающихся. Содержание дисциплины способствует правовому, экономическому, профессионально-трудовому, воспитанию обучающихся.

Реализация воспитательного потенциала дисциплины подразумевает:

– целенаправленный отбор преподавателем и включение в лекционный материал, материал для практических и (или) лабораторных занятий содержания, демонстрирующего обучающимся образцы настоящего научного подвижничества создателей и представителей данной отрасли науки (производства, экономики, культуры), высокого профессионализма ученых (представителей производства, деятелей культуры), их ответственности за результаты и последствия деятельности для человека и общества; примеры подлинной нравственности людей, причастных к развитию науки и производства;

– применение технологий, форм и методов преподавания дисциплины, имеющих высокий воспитательный эффект за счет создания условий для взаимодействия обучающихся с преподавателем, другими обучающимися, (командная работа, разбор конкретных ситуаций)*;*

– личный пример преподавателя, демонстрацию им в образовательной деятельности и общении с обучающимися за рамками образовательного процесса высокой общей и профессиональной культуры.

Реализация воспитательного потенциала дисциплины на учебных занятиях направлена на поддержание в университете единой развивающей образовательной и воспитательной среды. Реализация воспитательного потенциала дисциплины в ходе самостоятельной работы обучающихся способствует развитию в них целеустремленности, инициативности, креативности, ответственности за результаты своей работы – качеств, необходимых для успешной социализации и профессионального становления.

7. Фонд оценочных средств для проведения промежуточной аттестации

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

Таблица 7.1 – Этапы формирования компетенций

Код и содержание компетенции	Этапы формирования компетенций и дисциплины (модули), при изучении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
ПК-2.3 Проектирует детали и узлы биотехнических систем медицинского, экологического и биометрического назначения в соответствии с техническим заданием с использованием средств автоматизации проектирования	Информационные технологии Автоматизация обработки биомедицинской информации Теория алгоритмов и программирование для биотехнических систем Моделирование биологических процессов и систем	Язык СИ Прикладные пакеты математической обработки данных Методы обработки биомедицинских сигналов и данных Программное обеспечение сетевых технологий Основы информационной безопасности Теория и технология программирования для биотехнических систем	Объектно-ориентированное программирование Компьютерные технологии в медико-биологических исследованиях Системное программное обеспечение Медицинские информационные системы Введение в MATLAB Практика по получению первичных профессиональных умений и навыков Практика по получению профессиональных умений и опыта профессиональной деятельности
ПК-2.5 Контролирует оформление и соответствие законченных проектно-конструкторских работ, проектов и технической документации на изделия и устройства медицинского и экологического назначения нормативным документам	Информационные технологии для биотехнических систем Биофизические основы живых систем Информатика	Экология Управление в биотехнических системах Биотехнические системы медицинского назначения Научно-исследовательская работа Моделирование биологических	Системный анализ Методы проведения медико-биологических и экологических экспериментов Медицинские базы данных и экспертные системы Основы томографических исследований Математические основы компьютерной

	Электроды для измерения биоэлектрических потенциалов Биология Учебно-исследовательская работа Введение в направление подготовки и планирование профессиональной карьеры	процессов и систем Методы сбора и анализа медико-биологической информации Электрические характеристики биоматериалов Основы взаимодействия физических полей с биологическими объектами Введение в MATLAB Практика по получению первичных профессиональных умений и навыков	томографии Приборы и комплексы для лабораторного анализа Фотометрическая медицинская техника Преддипломная практика Научно-исследовательская работа Государственная итоговая аттестация

7.2. Описание показателей и критериев оценивания компетенций на раз- личных этапах их формирования, описание шкал оценивания

Таблица 7.2 – Показатели и критерии оценивания компетенций, шкала оценивания

Код компетенции/ этап *(указывается название этапа из п.7.1)*	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
ПК - 2 / основной	ПК-2.3 Проектирует детали и узлы биотехнически	**Знать**: простейшие методы работы с программным	**Знать**: принципы работы программных, программно-	**Знать**: принципы работы программных, программно-

Код компетенции/ этап *(указывается название этапа из п.7.1)*	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
	х систем медицинского, экологического и биометрического назначения в соответствии с техническим заданием с использованием средств автоматизации проектирования	обеспечением. **Владеть навыками**: сбора необходимой информации по работе с программными, программно-аппаратными средства информационной безопасности.	аппаратных средств и технических средств информационной безопасности **Уметь**: использовать навыки работы с компьютером при соблюдении основных требований информационной безопасности **Владеть навыками**: подбора наилучшего метода решения поставленной задачи	аппаратных средств и технических средств информационной безопасности **Уметь**: применять все полученные знания при решении разного рода задач по установке, настройке и обслуживанию программных, программно-аппаратных и технических средств защиты информации **Владеть навыками**: сбора достаточного количества информации для решения возникающих проблем профессионального характера
	ПК-2.5 Контролирует оформление и соответствие законченных проектно-конструкторских работ, проектов и технической	**Знать**: простейшие методы обработки результатов **Уметь**: выполнять научно-технические исследования с применением	**Знать**: принципы работы технических, программных и других средств информационной безопасности при проведении научно-технических	**Знать**: основные методы научно-технических исследований с применением средств информационной безопасности **Уметь**: применять все полученные

Код компетенции/ этап *(указывается название этапа из п.7.1)*	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
	документации на изделия и устройства медицинского и экологического назначения нормативным документам	технических средств и информационных технологий. **Владеть навыками**: проведения научно-технических исследований с применением технических средств обработки информации, информационных технологий в сфере информационной безопасности.	исследований **Уметь**: использовать навыки работы с техническими средствами обработки результатов при соблюдении основных требований информационной безопасности **Владеть навыками**: проведения научно-технических исследований и методами обработки результатов для подбора наилучшего метода решения задач информационной безопасности	знания для решении разного рода задач по установке, настройке и обслуживанию технических и программных средств обработки информации для проведения научно-технических исследований с применением средств информационной безопасности. **Владеть методами**: информационных технологий для проведения научно-технических исследований и построения систем информационной безопасности с применением технических средств

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

Таблица 7.3 – Паспорт комплекта оценочных средств для текущего контроля успеваемости

№ п/п	Раздел (тема) дисциплины	Код контролируемой компетенции (или её части)	Технология формирования	Оценочные средства		Описание шкал оценивания
				наименование	№№ заданий	
1	2	3	4	5	6	7
1	Введение в информационную безопасность	ПК-2.3	Лекция, СРС, практическое занятие	собеседование	1-7	Согласно табл.7.2
				тест	1-5	
2	Понятие защищенности в автоматизированных системах	ПК-2.3	Лекция, СРС, практическое занятие	собеседование	1-5	Согласно табл.7.2
				тест	1-4	
3	Основы законодательства РФ в области информационной безопасности и защиты информации	ПК-2.3	Лекция, СРС	собеседование	1-8	Согласно табл.7.2
4	Конфиденциальная информация и ее защита	ПК-2.3	Лекция, СРС	собеседование	1-7	Согласно табл.7.2

5	Лицензирование и сертификация в области обеспечения безопасности информации	ПК-2.3 ПК-2.5	Лекция, СРС	собеседование	1-8	Согласно табл.7.2
6	Технические средства обеспечения информационной безопасности	ПК-2.3 ПК-2.5	Лекция, СРС, практическое занятие	собеседование	1-8	Согласно табл.7.2
				тест	1-6	
7	Криптографические методы защиты информации	ПК – 2.5	Лекция, СРС, практическое занятие	собеседование	1-12	Согласно табл.7.2
				тест	1-4	
8	Каналы утечки информации	ПК – 2.3	Лекция, СРС, практическое занятие	собеседование	1-8	Согласно табл.7.2
				тест	1-6	
9	Угроза безопасности информации АСОД и субъектов информационных отношений	ПК-2.3 ПК-2.5	Лекция, СРС, практическое занятие	собеседование	1-9	Согласно табл.7.2
				тест	1-5	

Примеры типовых контрольных заданий для текущего контроля

Вопросы собеседования по разделу (теме) 4. «Конфиденциальная информация и ее защита»

1. Понятие конфиденциальной информации и ее виды.
2. Понятие коммерческая тайна.
3. Федеральный закон «О коммерческой тайне».
4. Понятие служебная тайна.
5. Понятие профессиональная тайна.
6. Понятие персональные данные.
7. Федеральный закон «О персональных данных».

Контрольные вопросы к практической работе по теме «Шифрование методом полиалфавитной замены»

1. На чем основан метод полиалфавитной замены?
2. Что такое матрица Вижинера?

3. Как строится матрица Вижинера?
4. Как осуществляется шифрование сообщения данным методом?
5. Как осуществляется расшифрование сообщения?

Типовые задания для проведения промежуточной аттестации обучающихся

Промежуточная аттестация по дисциплине проводится в форме зачета. Зачет проводится в виде компьютерного тестирования.

Для тестирования используются контрольно-измерительные материалы (КИМ) – вопросы и задания в тестовой форме, составляющие банк тестовых заданий (БТЗ) по дисциплине, утвержденный в установленном в университете порядке.

Проверяемыми на промежуточной аттестации элементами содержания являются темы дисциплины, указанные в разделе 4 настоящей программы. Все темы дисциплины отражены в КИМ в равных долях (%). БТЗ включает в себя не менее 100 заданий и постоянно пополняется. БТЗ хранится на бумажном носителе в составе УММ и электронном виде в ЭИОС университета.

Для проверки *знаний* используются вопросы и задания в различных формах:

- закрытой (с выбором одного или нескольких правильных ответов),
- открытой (необходимо вписать правильный ответ),
- на установление правильной последовательности,
- на установление соответствия.

Умения, навыки (или опыт деятельности) и компетенции проверяются с помощью компетентностно-ориентированных задач (ситуационных, производственных или кейсового характера) и различного вида конструкторов.

Все задачи являются многоходовыми. Некоторые задачи, проверяющие уровень сформированности компетенций, являются многовариантными. Часть умений, навыков и компетенций прямо не отражена в формулировках задач, но они могут быть проявлены обучающимися при их решении.

В каждый вариант КИМ включаются задания по каждому проверяемому элементу содержания во всех перечисленных выше формах и разного уровня сложности. Такой формат КИМ позволяет объективно определить качество освоения обучающимися основных элементов содержания дисциплины и уровень сформированности компетенций.

Примеры типовых заданий для проведения промежуточной аттестации обучающихся

Задание в закрытой форме:

Используя браузер, выполняется запрос методом ___.

Задание в открытой форме:

Вредоносные вставки при обращении к базе данных называются:

- инъекциями
- синхронизацией
-транзакциями

Задание на установление правильной последовательности

1. Выберите правильную последовательность этапов по созданию системы защиты персональных данных:
   a. Опытная и промышленная эксплуатация
   b. Проектный этап
   c. Аттестация или декларирование
   d. Предпроектный этап

Задание на установление соответствия:

1 Наиболее эффективный в системах обработки конфиденциальных данных алгоритм

2 Наиболее эффективный в системах реального времени алгоритм диспетчеризации

3 Наиболее просто реализуемый алгоритм

4 Алгоритм, позволяющий реализовывать динамические приоритеты

5 Алгоритм, при котором процесс может оставаться неограниченно долго в режиме ожидания

А "самый короткий - следующий"

Б алгоритм планирования согласно приоритетам

В "самый длинный - следующий"

Г выбор случайного процесса _____.

Компетентностно-ориентированная задача:

В качестве входной информации берется текстовый файл, состоящий из ФИО студента, названия кафедры и специальности. Исходный поток данных соответствует последовательности бит, расположение которых определяется формулой, учитывающей порядковый номер студента по списку.

$$ci = (7i+n) \bmod 13 + 13i$$

Ключ скремблера соответствует номеру зачетки студента «слева направо», генератор псевдослучайных чисел - аналогично «справа налево».

Порядок выполнения работы:

1. Сформировать блок исходных данных (не более 48 бит)
2. Рассчитать состояния скремблера для обработки входного блока
3. Рассчитать период зацикливания и период наибольшей длины скремблера.
4. Произвести скремблирование исходных данных.

5. Подобрать скремблер минимальной разрядности, который не зациклится при обработке всего исходного файла.

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

Процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, регулируются следующими нормативными актами университета:

- Положение П 02.016–2015 «О балльно-рейтинговой системе оценки качества освоения образовательных программ»;
- методические указания, используемые в образовательном процессе, указанные в списке литературы.

Для *текущего контроля* по дисциплине в рамках действующей в университете балльно-рейтинговой системы применяется следующий порядок начисления баллов:

Таблица 7.4 – Порядок начисления баллов в рамках БРС

Форма контроля	Минимальный балл		Максимальный балл	
	балл	примечание	балл	примечание
Выполнение работы «Шифрование методом простой замены»	2	Выполнил, но «не защитил»	4	Выполнил и «защитил»
Выполнение лабораторной работы «Шифрование методом полиалфавитной замены»	2	Выполнил, но «не защитил»	4	Выполнил и «защитил»
Защита работы «Шифрование методом перестановок»	2	Выполнил, но «не защитил»	4	Выполнил и «защитил»
Защита работы «Схема Шамира разделения секрета»	2	Выполнил, но «не защитил»	4	Выполнил и «защитил»
Выполнение лабораторной работы «Шифрование аналитическими методами (методами матричной алгебры)»	4	Выполнил, но «не защитил»	6	Выполнил и «защитил»
Выполнение работы по исследованию шифрования с открытым ключом	4	Выполнил, но «не защитил»	6	Выполнил и «защитил»
СРС	8		20	
Итого:	24		48	
Посещаемость	0		16	
Зачет	0		36	
Итого:	24		100	

Для *промежуточной аттестации*, проводимой в форме тестирования, используется следующая методика оценивания знаний, умений, навыков и (или) опыта деятельности. В каждом варианте КИМ – 16 заданий (15 вопросов и одна задача).

Каждый верный ответ оценивается следующим образом:

- задание в закрытой форме – 2 балла;
- задание в открытой форме – 2 балла;
- задание на установление правильной последовательности – 2 балла;
- задание на установление соответствия – 2 балла;
- решение задачи – 6 баллов.

Максимальное количество баллов за тестирование – 36 балов.

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

8.1. Основная литература

1. Технологии обеспечения безопасности информационных систем : учебное пособие : [16+] / А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов и др. – Москва ; Берлин : Директ-Медиа, 2021. – 210 с. : ил., схем., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=598988 (дата обращения: 07.09.2021). – Библиогр.: с. 196-205. – ISBN 978-5-4499-1671-6. – DOI 10.23681/598988. – Текст : электронный.

2. Основы информационной безопасности : учебник / В. Ю. Рогозин, И. Б. Галушкин, В. Новиков, С. Б. Вепрев ; Академия Следственного комитета Российской Федерации. – Москва : Юнити-Дана : Закон и право, 2018. – 287 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=562348 (дата обращения: 23.08.2021). – Библиогр. в кн. – ISBN 978-5-238-02857-6. – Текст : электронный.

3. Майстренко, Н. В. Основы теории информации и криптографии : учебное электронное издание / Н. В. Майстренко, А. В. Майстренко. – Тамбов : Тамбовский государственный технический университет (ТГТУ), 2018. – 81 с. : табл., граф., схем., ил. – URL: https://biblioclub.ru/index.php?page=book&id=570354 (дата обращения: 13.09.2021). – Библиогр. в кн. – ISBN 978-5-8265-1950-9. – Режим доступа: по подписке. – Текст : электронный.

8.2. Дополнительная литература

1. Романец, Ю. В. Защита информации в компьютерных системах и сетях / Ю. В. Романец, П. А. Тимофеев, В. Ф. Шаньгин. - 2-е изд., перераб. и доп. - М. : Радио и связь, 2001. - 376 с. : ил. - ISBN 5-256-01518-4. - Текст : непосредственный.

2. Левин, М. PGP. Кодирование и шифрование информации с открытым ключом / М. Левин. - М. : Майор, 2001. - 176 с. - Текст : непосредственный.

3. Иванов, М. А. Криптографические методы защиты информации в компьютерных системах и сетях / М. А. Иванов. - М. : КУДИЦ-ОБРАЗ, 2001. - 368 с. - Текст : непосредственный.

4. Основы криптографии : учеб. пособие / А. П. Алферов [и др.]. - М. : Гелиос АРВ, 2001. - 480 с. : ил. - Текст : непосредственный.

5. Галатенко, В. А. Основы информационной безопасности. Курс лекций : учебное пособие для студентов вузов / под ред. В. Б. Бетелина. - 2-е изд., испр. - М. : ИНТУИТ. РУ Интернет-университет Информационных Технологий, 2004. - 264 с. - (Основы информационных технологий). - Текст : непосредственный.

8.3. Перечень методических указаний

1) Шифрование методом прямой замены [Электронный ресурс] : методические указания по выполнению лабораторной работы по дисциплине «Введение в криптографию» для студентов специальностей 10.05.03, 10.05.02, 10.03.01 / Юго-Зап. гос. ун-т ; сост. М. А. Ефремов. - Электрон. текстовые дан. (240 КБ). - Курск : ЮЗГУ, 2016. - 14 с. : ил. - Библиогр.: с. 14. - Б. ц.

2) Шифрование методом полиалфавитной замены [Электронный ресурс] : методические указания по выполнению лабораторной работы по дисциплине «Введение в криптографию» для студентов специальностей 10.05.03, 10.05.02, 10.03.01 / Юго-Зап. гос. ун-т ; сост. М. А. Ефремов. - Электрон. текстовые дан. (294 КБ). - Курск : ЮЗГУ, 2016. - 9 с. : ил., табл. - Библиогр.: с. 9. - Б. ц.

3) Шифрование методом перестановок [Электронный ресурс] : методические указания по выполнению лабораторной работы по дисциплине «Введение в криптографию» для студентов специальностей 10.05.03, 10.05.02, 10.03.01 / Юго-Зап. гос. ун-т ; сост. М. А. Ефремов. - Электрон. текстовые дан. (223 КБ). - Курск : ЮЗГУ, 2016. - 9 с. : ил., табл. - Библиогр.: с. 9. - Б. ц.

4) Разделение секрета [Электронный ресурс] : методические указания по выполнению лабораторной работы по дисциплине «Криптографические методы защиты информации» для студентов специальностей 10.05.03, 10.05.02, 10.03.01 / Юго-Зап. гос. ун-т ; сост. М. А. Ефремов. - Электрон. текстовые дан. (552 КБ). - Курск : ЮЗГУ, 2016. - 13 с. - Библиогр.: с. 13. - Б. ц.

5) Шифрование аналитическими методами [Электронный ресурс] : методические указания по выполнению лабораторной работы по дисциплине «Введение в криптографию» для студентов специальностей 10.05.03, 10.05.02, 10.03.01 / Юго-Зап. гос. ун-т ; сост. М. А. Ефремов. - Электрон. текстовые дан. (333 КБ). - Курск : ЮЗГУ, 2016. - 11 с. - Б. ц.

6) Шифрование с открытым ключом [Электронный ресурс] : методические указания по выполнению лабораторной работы по дисциплине «Введение в криптографию» для студентов специальностей 10.05.03, 10.05.02, 10.03.01 / Юго-Зап. гос. ун-т ; сост. М. А. Ефремов. - Электрон. текстовые дан. (315 КБ). - Курск : ЮЗГУ, 2016. - 14 с. : ил. - Библиогр.: с. 14. - Б. ц.

9. Перечень ресурсов информационно-телекоммуникационной сети Интернет

1) http://biblioclub.ru - Электронно-библиотечная система «Университетская библиотека онлайн».
2) www.elibrary.ru/defaultx.asp - научная электронная библиотека.
3) www.edu.ru - федеральный портал «Российское образование».
4) www.consultant.ru - Официальный сайт компании «Консультант Плюс».
5) Федеральная служба безопасности [официальный сайт]. Режим доступа: http://www.fsb.ru/.
6) Научно-информационный портал ВИНИТИ РАН [официальный сайт]. Режим доступа: http://www.consultant.ru/

10. Методические указания для обучающихся по освоению дисциплины

Основными видами аудиторной работы студента при изучении дисциплины «Основы информационной безопасности» являются лекции и лабораторные занятия. Студент не имеет права пропускать занятия без уважительных причин.

На лекциях излагаются и разъясняются основные понятия темы, связанные с ней теоретические и практические проблемы, даются рекомендации для самостоятельной работы. В ходе лекции студент должен внимательно слушать и конспектировать материал.

Изучение наиболее важных тем или разделов дисциплины завершают лабораторные и практические занятия, которые обеспечивают: контроль подготовленности студента; закрепление учебного материала; приобретение опыта устных публичных выступлений, ведения дискуссии, в том числе аргументации и защиты выдвигаемых положений и тезисов.

Практическому занятию предшествует самостоятельная работа студента, связанная с освоением материала, полученного на лекциях, и материалов, изложенных в учебниках и учебных пособиях, а также литературе, рекомендованной преподавателем.

Качество учебной работы студентов преподаватель оценивает по результатам тестирования, собеседования, защиты отчетов по лабораторным и практическим работам.

Преподаватель уже на первых занятиях объясняет студентам, какие

формы обучения следует использовать при самостоятельном изучении дисциплины «Основы информационной безопасности»: конспектирование учебной литературы и лекции, составление словарей понятий и терминов и т. п.

В процессе обучения преподаватели используют активные формы работы со студентами: чтение лекций, привлечение студентов к творческому процессу на лекциях, промежуточный контроль путем отработки студентами пропущенных лекции, участие в групповых и индивидуальных консультациях (собеседовании). Эти формы способствуют выработке у студентов умения работать с учебником и литературой. Изучение литературы и справочной документации составляет значительную часть самостоятельной работы студента. Это большой труд, требующий усилий и желания студента. В самом начале работы над книгой важно определить цель и направление этой работы. Прочитанное следует закрепить в памяти. Одним из приемов закрепление освоенного материала является конспектирование, без которого немыслима серьезная работа над литературой. Систематическое конспектирование помогает научиться правильно, кратко и четко излагать своими словами прочитанный материал.

Самостоятельную работу следует начинать с первых занятий. От занятия к занятию нужно регулярно прочитывать конспект лекций, знакомиться с соответствующими разделами учебника, читать и конспектировать литературу по каждой теме дисциплины. Самостоятельная работа дает студентам возможность равномерно распределить нагрузку, способствует более глубокому и качественному усвоению учебного материала. В случае необходимости студенты обращаются за консультацией к преподавателю по вопросам дисциплины «Основы информационной безопасности» с целью усвоения и закрепления компетенций.

Основная цель самостоятельной работы студента при изучении дисциплины «Основы информационной безопасности» - закрепить теоретические знания, полученные в процессе лекционных занятий, а также сформировать практические навыки самостоятельного анализа особенностей дисциплины.

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

Microsoft Office 2016.Лицензионный договор №S0000000722 от 21.12.2015 г. с ООО «АйТи46», лицензионный договор №K0000000117 от 21.12.2015 г. с ООО «СМСКанал», Kaspersky Endpoint Security Russian Edition, лицензия 156A-140624-192234,Windows 7, договор IT000012385, Oracle Virtualbox (Бесплатная, GNU General Public License), редактор двоичных файлов Free Hex Editor Neo, (Свободное ПО http://www.hhdsoftware.com/free-hex-editor), открытая среда разработки

программного обеспечения Lazarus (Свободное ПО http://www.lazarus.freepascal.org/) ОС FreBSD (свободное ПО, лицензия BSD), ОС Ubuntu (Бесплатная, GNU GPLv3)

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

Учебная аудитория для проведения занятий лекционного типа и лаборатории кафедры информационной безопасности, оснащенные учебной мебелью: столы, стулья для обучающихся; стол, стул для преподавателя; доска. Компьютеры (10 шт.) CPU AMD-Phenom, ОЗУ 16 GB, HDD 2 Tb, монитор Aok 21”. Проекционный экран на штативе. Мультимедиацентр: ноутбук ASUSX50VLPMD-T2330/14"/1024Mb /160Gb/сумка/ проектор inFocusIN24+

13. Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

При обучении лиц с ограниченными возможностями здоровья учитываются их индивидуальные психофизические особенности. Обучение инвалидов осуществляется также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).

Для лиц с нарушением слуха возможно предоставление учебной информации в визуальной форме (краткий конспект лекций; тексты заданий, напечатанные увеличенным шрифтом), на аудиторных занятиях допускается присутствие ассистента, а также сурдопереводчиков и тифлосурдопереводчиков. Текущий контроль успеваемости осуществляется в письменной форме: обучающийся письменно отвечает на вопросы, письменно выполняет практические задания. Доклад (реферат) также может быть представлен в письменной форме, при этом требования к содержанию остаются теми же, а требования к качеству изложения материала (понятность, качество речи, взаимодействие с аудиторией и т. д.) заменяются на соответствующие требования, предъявляемые к письменным работам (качество оформления текста и списка литературы, грамотность, наличие иллюстрационных материалов и т.д.). Промежуточная аттестация для лиц с нарушениями слуха проводится в письменной форме, при этом используются общие критерии оценивания. При необходимости время подготовки к ответу может быть увеличено.

Для лиц с нарушением зрения допускается аудиальное предоставление информации, а также использование на аудиторных занятиях звукозаписывающих устройств (диктофонов и т.д.). Допускается присутствие на занятиях ассистента (помощника), оказывающего обучающимся необходимую техническую помощь. Текущий контроль успеваемости осуществляется в устной форме. При проведении промежуточной аттестации

для лиц с нарушением зрения тестирование может быть заменено на устное собеседование по вопросам.

Для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, на аудиторных занятиях, а также при проведении процедур текущего контроля успеваемости и промежуточной аттестации могут быть предоставлены необходимые технические средства (персональный компьютер, ноутбук или другой гаджет); допускается присутствие ассистента (ассистентов), оказывающего обучающимся необходимую техническую помощь (занять рабочее место, передвигаться по аудитории, прочитать задание, оформить ответ, общаться с преподавателем).