Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Усынин Максим Валерьевич
Должность: Ректор
Дата подписания: 17.08.2023 11:56:07
Уникальный программный ключ:
f498e59e83f65dd7c3ce7bb8a25cbbabb33ebc58

Частное образовательное учреждение высшего образования
«Международный Институт Дизайна и Сервиса»
(ЧОУВО МИДиС)

Кафедра математики и информатики

УТВЕРЖДАЮ
Ректор
М.В. Усынин
«29» мая 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Направление подготовки 09.03.03 Прикладная информатика
Направленность (профиль): Разработка Web и мобильных приложений
Квалификация выпускника: бакалавр
Форма обучения: очная
Год набора – 2021

Челябинск 2023

Рабочая программа дисциплины «Информационная безопасность» разработана на основе Федерального государственного образовательного стандарта высшего образования по направлению подготовки 09.03.03 Прикладная информатика (уровень бакалавриата) (Приказ Министерства образования и науки РФ 19 сентября 2017 г. N 922)

Автор-составитель: Статных А.С.

Рабочая программа рассмотрена и утверждена на заседании кафедры математики и информатики. Протокол № 10 от 29.05.2023

Заведующий кафедрой математики и информатики, к.т.н. Л.Ю. Овсяницкая

СОДЕРЖАНИЕ

1. Наименование дисциплины (модуля), цель и задачи освоения дисциплины (модуля).....4
2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы.....4
3. Место дисциплины (модуля) в структуре образовательной программы.....5
4. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающегося с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся.....5
5. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий.....5
6. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю).....13
7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля).....13
8. Перечень ресурсов информационно-телекоммуникационной сети «интернет», необходимых для освоения дисциплины (модуля).....14
9. Методические указания для обучающихся по освоению дисциплины (модуля).....14
10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения, современных профессиональных баз данных и информационных справочных систем 17
11. Материально-техническая база, необходимая для осуществления образовательного поцесса по дисциплине (модулю).....18

1. НАИМЕНОВАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ), ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

1.1. Наименование дисциплины

Информационная безопасность

1.2. Цель дисциплины

Формирование у обучаемых знаний в области теоретических основ информационной безопасности и навыков практического обеспечения защиты информации и безопасного использования программных средств в вычислительных системах.

1.3. Задачи дисциплины

- научиться реализовывать мероприятия для обеспечения на предприятии (в организации) деятельности в области защиты информации;
- проводить анализ степени защищенности информации и осуществлять повышение уровня защиты с учетом развития математического и программного обеспечения вычислительных систем;
- применять средства и системы защиты информации.

2. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс изучения дисциплины «Информационная безопасность» направлен на формирование следующих компетенций:

Код и наименование компетенций выпускника	Код и наименование индикатора достижения компетенций
ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-3.1. Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности ОПК-3.2. Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности ОПК-3.3. Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности
ОПК-4. Способен участвовать в разработке стандартов, норм, правил, а также технической документации, связанной с профессиональной деятельностью	ОПК-4.1. Знает основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы ОПК-4.2. Умеет применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы ОПК-4.3. Владеет навыками составления технической документации на различных этапах жизненного цикла информационной системы

3. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Учебная дисциплина «Информационная безопасность» относится к обязательной части учебного плана по основной профессиональной образовательной программе по направлению подготовки 09.03.03 Прикладная информатика, направленность (профиль) Разработка Web и мобильных приложений.

4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ) В ЗАЧЕТНЫХ ЕДИНИЦАХ С УКАЗАНИЕМ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ, ВЫДЕЛЕННЫХ НА КОНТАКТНУЮ РАБОТУ ОБУЧАЮЩЕГОСЯ С ПРЕПОДАВАТЕЛЕМ (ПО ВИДАМ УЧЕБНЫХ ЗАНЯТИЙ) И НА САМОСТОЯТЕЛЬНУЮ РАБОТУ ОБУЧАЮЩИХСЯ

Общая трудоемкость (объем) дисциплины составляет 4 зачетных единицы, 144 академических часов. Дисциплина изучается на 4 курсе, 7 семестре.

Вид учебной работы	Всего	Разделение по семестрам
		7
Общая трудоемкость, ЗЕТ	**4**	**4**
Общая трудоемкость, час.	144	144
Аудиторные занятия, час.	64	64
Лекции, час.	32	32
Практические занятия, час.	32	32
Самостоятельная работа	80	80
Курсовой проект (работа)	-	-
Контрольные работы	-	-
Вид итогового контроля	Зачет	Зачет

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ), СТРУКТУРИРОВАННОЕ ПО ТЕМАМ (РАЗДЕЛАМ) С УКАЗАНИЕМ ОТВЕДЕННОГО НА НИХ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ И ВИДОВ УЧЕБНЫХ ЗАНЯТИЙ

5.1. Содержание дисциплины

РАЗДЕЛ 1. ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ТЕМА 1.1. Основные положения теории информации

Определение информации. Виды информации, типы каналов связи. Схема канала связи по Шеннону. Особенности и технические характеристики современных каналов передачи информации, использующих различные физические принципы (электрические, акустические, оптические, радиочастотные) с точки зрения безопасности. Элементы теории кодирования. Виды сигналов, преимущества цифровых каналов перед аналоговыми с точки зрения защищённости передаваемой информации.

ТЕМА 1.2. Правовое регулирование информационных процессов в обществе

1. Важность и ценность информации. Виды информации, подлежащие защите. Классификация информации по степени ограниченности доступа к ней (открытая, конфиденциальная, секретная).

2. Понятие тайны (государственная, промышленная, коммерческая, финансовая, частная тайна).

3. Государство как гарант права граждан на защиту личной информации и интеллектуальной собственности. Законы Российской Федерации о защите тайны и интеллектуальной собственности.

ТЕМА 1.3. Методы похищения, искажения, подмены, уничтожения информации

1. Виды информационных нападений (по месту воздействия): на каналы связи, на оконечные устройства каналов связи-преобразователи информации, на объект - носитель информации.

2. Виды информационных нападений (по способу воздействия): пассивные, активные. Виды методов. Традиционные методы с использованием подручных технических средств.

ТЕМА 1.4. Устройства двойного применения.

1. Использование возможностей современной техники для получения стабильного результата. Использование существующих каналов связи (телефонные - проводные и беспроводные, электросети, кабельные системы, радиотрансляционные сети, каналы радиовещания и телевизионные каналы, оптические, акустические) и оконечных устройств (телефонные аппараты, факсы, телевизоры, радиоприёмники, бытовые электроприборы, ПЭВМ).

2. Использование свойств обратимости преобразователей информации. Организация новых каналов на базе существующих (внедрение дополнительных преобразователей) или самостоятельных.

3. Радиоэлектронные средства. Электронные устройства двойного применения. Использование средств спецтехники.

РАЗДЕЛ 2. ОБЩИЕ ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ТЕМА 2.1. Информационная безопасность и современные информационные технологии

1. Понятие информационной среды общества и информационной безопасности. Концепция информационной безопасности Российской Федерации в основных сферах: политической, экономической, военной, в сфере духовной жизни.

2. Основной понятийный аппарат информационной безопасности: защита информации; информационная инфраструктура; угрозы информационной безопасности; несанкционированный доступ к информации.

3. Классификация источников угроз информационной безопасности: внешние; внутренние. Классификация информационных угроз по способам воздействия на объекты ИБ: информационные; программно математические; физические; радиоэлектронные; организационно-правовые. Последствия воздействия угроз на различных уровнях (государство, общество, отдельные граждане).

4. Основные объекты информационной безопасности и специфика угроз для них: в общегосударственных информационных и телекоммуникационных системах; в области науки и техники; в сфере экономики.

5. Комплекс мероприятий по обеспечению информационной безопасности объектов электронно-вычислительной техники: организационно-административные мероприятия; технические мероприятия и методы; программные методы.

ТЕМА 2.2. Общие принципы системного подхода к обеспечению безопасности информации

1. Организационные меры для выявления и предотвращения угроз информационной безопасности. Понятие о сертификации информационных устройств. Физические меры (пространственное отделение и защита объекта - носителя информации).

2. Закрытие каналов передачи (шифрование), использование современных каналов связи с наибольшим уровнем скрытности и помехозащищенности. Виды устройств шифрования (канальные, абонентские).

ТЕМА 2.3. Безопасность компьютерных систем.

1. ПЭВМ и компьютерные сети - общие принципы построения, схемы потоков информации, выявление возможных точек и каналов для информационных угроз, возможные меры по их устранению или блокированию.

2. Влияние архитектуры ЭВМ на безопасность обрабатываемой информации. Понятие "защищённая архитектура". Операционные системы, ориентированные на безопасность информации.

3. Безопасность компьютерных сетей - корпоративных и глобальных (общие принципы). Компьютерные вирусы.

4. Стандартные средства защиты (аппаратные и программные). Дополнительные средства: аппаратные средства закрытия (шифрование, противодействие перехвату), программные средства (программы шифрования, разграничение доступа к данным). Организационные меры по защите информации на ЭВМ.

5. Преобразования секретной информации (криптография). Традиционные методы. Методы, ориентированные на использование ЭВМ. Методы, основанные на аппаратных средствах.

6. Стандарты шифрования. Использование криптографических методов для защиты электронной документации. Электронная цифровая подпись - технология применения и защита.

ТЕМА 2.4. Противоправное использование компьютеров

1. Сущность компьютерных преступлений. Расшифровка термина "компьютерная преступность". Классификация компьютерных преступлений. Кодификатор Генерального Секретариата Интерпола.

2. Основные виды компьютерных преступлений: компьютерные экономические преступления; преступления, связанные с нарушением частной тайны; компьютерные преступления против "неиндивидуальных" интересов. Тенденции развития компьютерной преступности.

3. "Электронные деньги" и безопасность платёжных систем с использованием пластиковых карт.

5.2. Тематический план

Номера и наименование разделов и тем	Количество часов				
	Общая трудоёмкость	из них			
		Самостоятельная работа	Аудиторные занятия	из них	
				Лекции	Практические занятия
Раздел I. ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ					
Тема 1.1.Основные положения теории информации	18	10	8	4	4
Тема 1.2. Правовое регулирование информационных процессов в обществе	18	10	8	4	4
Тема 1.3. Методы похищения, искажения, подмены, уничтожения информации	18	10	8	4	4
Тема 1.4. Устройства двойного применения	18	10	8	4	4
Итого раздел I	**72**	**40**	**32**	**16**	**16**
Раздел 2. ОБЩИЕ ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ					
Тема 2.1. Информационная безопасность и современные информационные технологии	18	10	8	4	4
Тема 2.2. Общие принципы системного подхода к обеспечению безопасности информации	18	10	8	4	4
Тема 2.3. Безопасность компьютерных систем	18	10	8	4	4

Тема 2.4. Противоправное использование компьютеров	18	10	8	4	4
Итого раздел 2	**72**	**40**	**32**	**16**	**16**
Всего изучено по дисциплине	**144**	**80**	**64**	**32**	**32**
Всего зачетных единиц	**4**				

5.3. Лекционные занятия

Тема	Содержание	час.	Формируемые компетенции
Раздел I. ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ			
Тема 1.1. Основные положения теории информации	Определение информации. Виды информации, типы каналов связи. Схема канала связи по Шеннону. Особенности и технические характеристики современных каналов передачи информации, использующих различные физические принципы (электрические, акустические, оптические, радиочастотные) с точки зрения безопасности. Элементы теории кодирования. Виды сигналов, преимущества цифровых каналов перед аналоговыми с точки зрения защищённости передаваемой информации.	4	ОПК-3 ОПК-4
Тема 1.2. Правовое регулирование информационных процессов в обществе	Важность и ценность информации. Виды информации, подлежащие защите. Классификация информации по степени ограниченности доступа к ней (открытая, конфиденциальная, секретная). Понятие тайны (государственная, промышленная, коммерческая, финансовая, частная тайна). Государство как гарант права граждан на защиту личной информации и интеллектуальной собственности. Законы Российской Федерации о защите тайны и интеллектуальной собственности.	4	ОПК-3 ОПК-4
Тема 1.3. Методы похищения, искажения, подмены, уничтожения информации	Виды информационных нападений (по месту воздействия): на каналы связи, на оконечные устройства каналов связи-преобразователи информации, на объект - носитель информации. Виды информационных нападений (по способу воздействия): пассивные, активные. Виды методов. Традиционные методы без использования технических средств. Традиционные методы с использованием подручных технических средств.	4	ОПК-3 ОПК-4
Тема 1.4. Устройства двойного применения	Использование возможностей современной техники для получения стабильного результата. Использование существующих каналов связи (телефонные - проводные и беспроводные, электросети, кабельные системы, радиотрансляционные сети, каналы радиовещания и телевизионные каналы, оптические, акустические) и оконечных устройств (телефонные аппараты, факсы, телевизоры, радиоприёмники, бытовые электроприборы, ПЭВМ).	4	ОПК-3 ОПК-4

	Использование свойств обратимости преобразователей информации. Организация новых каналов на базе существующих (внедрение дополнительных преобразователей) или самостоятельных. Радиоэлектронные средства. Электронные устройства двойного применения. Использование средств спецтехники.		
Раздел 2. ОБЩИЕ ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ			
Тема 2.1. Информационная безопасность и современные информационные технологии	Понятие информационной среды общества и информационной безопасности. Концепция информационной безопасности Российской Федерации в основных сферах: политической, экономической, военной, в сфере духовной жизни. Основной понятийный аппарат информационной безопасности: защита информации; информационная инфраструктура; угрозы информационной безопасности; несанкционированный доступ к информации. Классификация источников угроз информационной безопасности: внешние; внутренние. Классификация информационных угроз по способам воздействия на объекты ИБ:информациионные;программно-математи-ческие; физические;радиоэлектронные;организационно-правовые.Последствия воздействия угроз на различных уровнях (государство, общество, отдельные граждане). Основные объекты информационной безопасности и специфика угроз для них: в общегосударственных информационных и телекоммуникационных системах; в области науки и техники; в сфере экономики. Комплекс мероприятий по обеспечению информационной безопасности объектов электронно-вычислительной техники: организационно-административные мероприятия; технические мероприятия и методы; программные методы.	4	ОПК-3 ОПК-4
Тема 2.2. Общие принципы системного подхода к обеспечению безопасности информации	. Организационные меры для выявления и предотвращения угроз информационной безопасности. Понятие о сертификации информационных устройств. Физические меры (пространственное отделение и защита объекта - носителя информации). Закрытие каналов передачи (шифрование), использование современных каналов связи с наибольшим уровнем скрытности и помехозащищенности. Виды устройств шифрования (канальные, абонентские). Тестирование каналов связи. Средства противодействия (активные и пассивные). Технические средства защиты (по принципу действия).	4	ОПК-3 ОПК-4
Тема 2.3. Безопасность компьютерных систем	ПЭВМ и компьютерные сети - общие принципы построения, схемы потоков информации, выявление возможных точек и каналов для информационных угроз, возможные меры по их устранению или блокированию.	4	ОПК-3 ОПК-4

	Влияние архитектуры ЭВМ на безопасность обрабатываемой информации. Понятие "защищённая архитектура". Операционные системы, ориентированные на безопасность информации. Безопасность компьютерных сетей - корпоративных и глобальных (общие принципы). Компьютерные вирусы. Стандартные средства защиты (аппаратные и программные). Дополнительные средства: аппаратные средства закрытия (шифрование, противодействие перехвату), программные средства (программы шифрования, разграничение доступа к данным). Организационные меры по защите информации на ЭВМ. Преобразования секретной информации (криптография). Традиционные методы. Методы, ориентированные на использование ЭВМ. Методы, основанные на аппаратных средствах.		
Тема 2.4. Противоправное использо-вание компью-теров	Сущность компьютерных преступлений. Расшифровка термина "компьютерная преступность". Классификация компьютерных преступлений. Кодификатор Генерального Секретариата Интерпола. Основные виды компьютерных преступлений: компьютерные экономические преступления; преступления, связанные с нарушением частной тайны; компьютерные преступления против "неиндивидуальных" интересов. Тенденции развития компьютерной преступности. Электронные деньги" и безопасность платёжных систем с использованием пластиковых карт.	4	ОПК-3 ОПК-4

5.4. Практические занятия

Тема	Содержание	час.	Формируемые компетенции	Методы и формы контроля формируемых компетенций
Раздел I. ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ				
Тема 1.1. Основные положения теории информации	Информационная безопасность и современные информационные технологии. Применение электронных устройств двойного назначения.	4	ОПК-3 ОПК-4	Тестирование
Тема 1.2. Правовое регулирование информационных процессов в обществе	Сущность компьютерных преступлений. Расшифровка термина "компьютерная преступность". Классификация компьютерных преступлений.	4	ОПК-3 ОПК-4	Тестирование
Тема 1.3. Методы похищения,	Безопасность компьютерных систем.ПЭВМ и компьютерные сети - общие	4	ОПК-3 ОПК-4	Проверка практических работ

искажения, подмены, уничтожения информации	принципы построения, схемы потоков информации, выявление возможных точек и каналов для информационных угроз, возможные меры по их устранению или блокированию. Влияние архитектуры ЭВМ на безопасность обрабатываемой информации. Понятие "защищённая архитектура". Операционные системы, ориентированные на безопасность информации. Безопасность компьютерных сетей - корпоративных и глобальных (общие принципы). Компьютерные вирусы.			
Тема 1.4. Устройства двойного применения	Виды информационных нападений (по месту воздействия): на каналы связи, на оконечные устройства каналов связи-преобразователи информации, на объект - носитель информации Виды информационных нападений (по способу воздействия): пассивные, активные. Виды методов. Традиционные методы без использования технических средств. Традиционные методы с использованием подручных технических средств.	4	ОПК-3 ОПК-4	Проверка Индивидуальных Заданий промежуточного контроля
Раздел 2. ОБЩИЕ ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ				
Тема 2.1. Информационная безопасность и современные информационные технологии	Преобразования секретной информации (криптография). Традиционные методы. Методы, ориентированные на использование ЭВМ. Методы, основанные на аппаратных средствах. Стандарты шифрования. Использование криптографических методов для защиты электронной документации. Электронная цифровая подпись - технология применения и защита.	4	ОПК-3 ОПК-4	Тестирование, Проверка практических работ
Тема 2.2. Общие принципы системного подхода к обеспечению безопасности информации	Правовое регулирование информационных процессов в обществе. Важность и ценность информации. Виды информации, подлежащие защите. Классификация информации по степени ограниченности доступа к ней (открытая, конфиденциальная, секретная). Понятие тайны (государственная, промышленная, коммерческая, финансовая, частная тайна). Государство как гарант права граждан на защиту личной информации и интеллектуальной собственности. Законы Российской Федерации о защите тайны и интеллектуальной собственности.	4	ОПК-3 ОПК-4	Тестирование, Проверка практических работ

Тема 2.3. Безопасность компьютерных систем	Сетевые сканеры и мониторинг компьютерных сетей	4	ОПК-3 ОПК-4	Тестирование, Проверка практических работ
Тема 2.4. Противоправное использование компьютеров	Основные виды компьютерных преступлений: компьютерные экономические преступления; преступления, связанные с нарушением частной тайны; компьютерные преступления против "неиндивидуальных" интересов. Тенденции развития компьютерной преступности.	4	ОПК-3 ОПК-4	Тестирование, Проверка практических работ

5.5. Самостоятельная работа обучающихся

Тема	Виды самостоятельной работы	Формируемые компетенции	Методы и формы контроля формируемых компетенций	часы
Раздел I. ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ				
Тема 1.1. Основные положения теории информации	1. Подготовка вопросов для практического занятия на основе изучения основной и дополнительной литературы 2. Работа по теме доклада	ОПК-3 ОПК-4	Проверка выполнения заданий для самостоятельной работы студентов	8
Тема 1.2. Правовое регулирование информационных процессов в обществе	1. Подготовка вопросов для практического занятия на основе изучения основной и дополнительной литературы 2. Выполнение домашнего задания по теме	ОПК-3 ОПК-4	Выполнение реферата	8
Тема 1.3. Методы похищения, искажения, подмены, уничтожения информации	1. Подготовка вопросов для практического занятия на основе изучения основной и дополнительной литературы 2. Выполнение домашнего задания по теме	ОПК-3 ОПК-4	Проверка выполнения заданий для самостоятельной работы студентов	8
Тема 1.4. Устройства двойного применения	1. Подготовка вопросов для практического занятия на основе изучения основной и дополнительной литературы. 2. Выполнение домашнего задания по теме	ОПК-3 ОПК-4	Проверка выполнения заданий для самостоятельной работы студентов	8
Раздел 2. ОБЩИЕ ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ				
Тема 2.1. Информационная безопасность и совре-	1. Подготовка вопросов для практического занятия на основе изучения основной и дополнительной литературы.	ОПК-3 ОПК-4	Проверка выполнения заданий для са-	8

менные информационные технологии	2. Выполнение домашнего задания по теме		мостоятельной работы студентов	
Тема 2.2. Общие принципы системного подхода к обеспечению безопасности информации	1. Подготовка вопросов для практического занятия на основе изучения основной и дополнительной литературы. 2. Выполнение домашнего задания по теме	ОПК-3 ОПК-4	Проверка выполнения заданий для самостоятельной работы студентов	8
Тема 2.3. Безопасность компьютерных систем	1. Подготовка вопросов для практического занятия на основе изучения основной и дополнительной литературы. 2. Выполнение домашнего задания по теме	ОПК-3 ОПК-4	Проверка выполнения заданий для самостоятельной работы студентов	8
Тема 2.4. Противоправное использование компьютеров	1. Подготовка вопросов для практического занятия на основе изучения основной и дополнительной литературы. 2. Выполнение домашнего задания по теме	ОПК-3 ОПК-4	Проверка выполнения заданий для самостоятельной работы студентов	8

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Фонд оценочных средств (ФОС) по дисциплине «Информационная безопасность» представлен отдельным документом и является частью рабочей программы

7. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ УЧЕБНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

Основная литература:

Электронные издания (электронные ресурсы)

1. Богатырев, В.А. Информационные системы и технологии. Теория надежности: учебное пособие для вузов / В.А. Богатырев. — Москва: Юрайт, 2022. — 318 с. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/490026 (дата обращения: 17.05.2023).

2. Зенков, А.В. Информационная безопасность и защита информации: учебное пособие для вузов / А.В. Зенков. — 2-е изд., перераб. и доп. — Москва: Юрайт, 2023. — 107 с. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/530927 (дата обращения: 17.05.2023).

3. Казарин, О.В. Надежность и безопасность программного обеспечения: учебное пособие для вузов / О.В. Казарин, И.Б. Шубинский. — Москва: Юрайт, 2023. — 342 с. . — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/515435 (дата обращения: 17.05.2023).

4. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для вузов / под ред. Т.А. Поляковой, А.А. Стрельцова. — Москва: Юрайт, 2023. — 325 с. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/511239 (дата обращения: 17.05.2023).

5. Фомичёв, В.М. Криптографические методы защиты информации в 2 ч.: учебник для вузов / В.М. Фомичёв, Д.А. Мельников ; под ред. В.М. Фомичёва. — Москва: Юрайт,

2023. — 209 с. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/511700 (дата обращения: 17.05.2023).

Дополнительные источники *(при необходимости)*

1. Внуков, А.А. Защита информации : учебное пособие для вузов / А.А. Внуков. — 3-е изд., перераб. и доп. — Москва: Юрайт, 2023. — 161 с. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/512268 (дата обращения: 17.05.2023).

2. Партыка, Т.Л. Информационная безопасность [Текст]: учеб. пособие для вузов, спо/Т.Л.Партыка, И.И.Попов. – М.: ФОРУМ:ИНФРА-М, 2016.-368с.: ил.

3. Щеглов, А.Ю. Защита информации: основы теории: учебник для вузов / А.Ю. Щеглов, К.А. Щеглов. — Москва: Юрайт, 2023. — 309 с. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/511998 (дата обращения: 17.05.2023).

4. Якушева, Н.М. Вычислительные системы, сети и телекоммуникации [Текст]: учеб. Пособие / Н.М.Якушева. – М.: Спутник +, 2014. – 304 с.

8. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫХ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

Для выполнения заданий, предусмотренных рабочей программой используются рекомендованные Интернет-сайты, ЭБС.

Электронные образовательные ресурсы

1. Образовательная платформа ЮРАЙТ http://www.urait.ru;
2. http://bezopasnik.org/article/1.htm;
3. https://sites.google.com/site/anisimovkhv/learning/kripto/lecture/

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Содержание методических рекомендаций включает:

- цели и задачи изучения дисциплины;
- структура курса и конкретизированы отдельные модули, составляющие курс
- советы по планированию и организации времени, отведенного на изучение дисциплины;
- описание последовательности действий студента, или «сценарий изучения дисциплины»;
- рекомендации по использованию материалов учебно-методического комплекса;
- рекомендации по работе с литературой;
- советы по подготовке к экзамену;
- разъяснения по поводу работы с тестовой системой курса, по выполнению домашних заданий и т.д.

1. **Советы по планированию и организации времени, необходимого для изучения дисциплины «Информационная безопасность».** Рекомендуется следующим образом организовать время, необходимое для изучения дисциплины:

Работа с литературой – 1 час в неделю

Подготовка к практическому занятию – не менее 1 час.

Подготовка к зачету – не менее 5 часов.

2. Описание последовательности действий студента («сценарий изучения дисциплины»).

Для понимания материала и качественного его усвоения рекомендуется следующая последовательность действий:

1. В течение недели выбрать время для работы с литературой по вычислительной технике и операционным системам.

2. При подготовке к занятиям следующего дня, необходимо прочитать основные понятия по теме домашнего задания.

3. Рекомендации по использованию материалов рабочей программы.

Рекомендуется использовать текст лекций преподавателя, пользоваться рекомендациями по изучению дисциплины; использовать литературу, рекомендуемую составителями программы; использовать вопросы к зачету, примерные контрольные работы. Учесть требования, предъявляемые к студентам и критерии оценки знаний.

4. Указания по организации работы с контрольно-измерительными материалами, по выполнению домашних заданий.

При выполнении домашних заданий необходимо сначала прочитать основные понятия по теме домашнего задания. При выполнении упражнения или задачи нужно сначала понять, что требуется в задаче, какой теоретический материал нужно использовать, наметить план решения задачи. Если это не дало результатов, и Вы сделали задачу «по образцу» аудиторной задачи, или из методического пособия, нужно после решения такой задачи обдумать ход решения и попробовать решить аналогичную задачу самостоятельно.

6. Советы при подготовке к зачету.

При подготовке к экзаменам следует в первую очередь обратить внимание на определения основных понятий курса, формулировки основных определений. Определение должно формулироваться точно, любая неточность в формулировке определения, как правило, приводит к тому, что оно становится неверным. То же самое можно сказать и о формулировках теорем и других предложений курса.

Во время сдачи зачета (теста) для успешного выполнения индивидуального задания, оптимальна следующая стратегия: последовательно читайте условия задач и, если есть уверенность, что умеете ее решать – решайте, если ли есть сомнения, то переходите к следующей. Все «пропущенные» задачи пройдете второй раз. Если после второго прохода остались «белые пятна», то не следует заполнять их наугад. И не забывайте о том, что задачи часто имеют «подводные камни».

7. Советы по организации самостоятельной работы.

В связи с введением в образовательный процесс нового Федерального государственного образовательного стандарта все более актуальной становится задача организации самостоятельной работы студентов. Самостоятельная работа определяется как индивидуальная или коллективная учебная деятельность, осуществляемая без непосредственного руководства педагога, но по его заданиям и под его контролем.

Самостоятельная работа заключается в изучении отдельных тем курса по заданию преподавателя по рекомендуемой им учебной литературе, в решении заданий, решении кейс-задач, решении разноуровневых задач и заданий, выполнении расчетно-графических работ, в подготовке к контрольным работам, к устным ответам на практическом занятии; к докладам, сообщениям по теме, к докладам по проектам. Самостоятельная работа, включает освоение теоретической составляющей и выполнение расчётных задач.

Самостоятельная работа студентов является одной из основных форм внеаудиторной работы при реализации учебных планов и программ. По дисциплине «Информационная безопасность» практикуются следующие виды и формы самостоятельной работы студентов:

- отработка изучаемого материала по печатным и электронным источникам, конспектам лекций;

- изучение лекционного материала по электронному конспекту с использованием рекомендованной литературы;

- завершение практических работ и оформление отчётов;

- подготовка информационных сообщений, докладов с компьютерной презентацией, рефератов;

- подготовка материала-презентации.

Целью самостоятельной работы студентов является овладение фундаментальными знаниями, профессиональными умениями и навыками деятельности по профилю, опытом творческой, исследовательской деятельности.

Самостоятельная работа студентов способствует развитию самостоятельности, ответственности и организованности, творческого подхода к решению проблем учебного и профессионального уровня.

Студент в процессе обучения должен не только освоить учебную программу, но и приобрести навыки самостоятельной работы. Студенту предоставляется возможность работать во время учебы более самостоятельно, чем учащимся в средней школе. Студент должен уметь планировать и выполнять свою работу.

Самостоятельная работа студентов является обязательной для каждого студента и определяется учебным планом.

При определении содержания самостоятельной работы студентов следует учитывать их уровень самостоятельности и требования к уровню самостоятельности выпускников для того, чтобы за период обучения искомый уровень был достигнут.

Для организации самостоятельной работы необходимы следующие условия:

-готовность студентов к самостоятельному труду;

- наличие и доступность необходимого учебно-методического и справочного материала;

- консультационная помощь.

Формы самостоятельной работы студентов определяются при разработке рабочих программ учебных дисциплин содержанием учебной дисциплины, учитывая степень подготовленности студентов.

2. Виды самостоятельных работ

В учебном процессе выделяют два вида самостоятельной работы: - аудиторная; - внеаудиторная.

Аудиторная самостоятельная работа по дисциплине выполняется на учебных занятиях под непосредственным руководством преподавателя и по его заданию.

Внеаудиторная самостоятельная работа выполняется студентом по заданию преподавателя, но без его непосредственного участия.

Содержание внеаудиторной самостоятельной определяется в соответствии с рекомендуемыми видами заданий согласно примерной и рабочей программ учебной дисциплины.

Согласно Положению об организации внеаудиторной самостоятельной работы студентов на основании компетентностного подхода к реализации профессиональных образовательных программ, видами заданий для внеаудиторной самостоятельной работы являются:

-для овладения знаниями: чтение текста (учебника, первоисточника, дополнительной литературы), составление плана текста, графическое изображение структуры текста, конспектирование текста, выписки из текста, работа со словарями и справочниками, ознакомление с нормативными документами, учебно-исследовательская работа, использование аудио- и видеозаписей, компьютерной техники и Интернета и др.

-для закрепления и систематизации знаний: работа с конспектом лекции, обработка текста, повторная работа над учебным материалом (учебника, первоисточника, дополнительной литературы, аудио и видеозаписей, составление плана, составление таблиц для систематизации учебного материала, ответ на контрольные вопросы, заполнение рабочей тетради, аналитическая обработка текста (аннотирование, рецензирование, реферирование, конспект-анализ и др), завершение аудиторных практических работ и оформление отчётов

по ним, подготовка мультимедиа сообщений/докладов к выступлению на семинаре (конференции), материалов-презентаций, подготовка реферата, составление библиографии, тематических кроссвордов, тестирование и др.

-для формирования умений: решение задач и упражнений по образцу, решение вариативных задач, выполнение чертежей, схем, выполнение расчетов (графических работ), решение ситуационных (профессиональных) задач, подготовка к деловым играм, проектирование и моделирование разных видов и компонентов профессиональной деятельности, опытно экспериментальная работа, рефлексивный анализ профессиональных умений с использованием аудио- и видеотехники и др.

Самостоятельная работа может осуществляться индивидуально или группами студентов в зависимости от цели, объема, конкретной тематики самостоятельной работы, уровня сложности, уровня умений студентов.

Контроль результатов внеаудиторной самостоятельной работы студентов может осуществляться в пределах времени, отведенного на обязательные учебные занятия по дисциплине и внеаудиторную самостоятельную работу студентов по дисциплине, может проходить в письменной, устной или смешанной форме.

Виды внеаудиторной самостоятельные работы студентов:

- подготовка докладов и информационных сообщений на заданные темы и их слайдового сопровождения;
- подготовка и написание рефератов;
- завершение практических работ и оформление отчётов;
- написание конспекта первоисточника;
- создание материала-презентации.

Чтобы развить положительное отношение студентов к внеаудиторной самостоятельные работы студентов, следует на каждом ее этапе разъяснять цели работы, контролировать понимание этих целей студентами, постепенно формируя у них умение самостоятельной постановки задачи и выбора цели.

Оценка успешности ведется в традиционной системе: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно»- и отражается в электронном журнале, рассчитывается по формуле, в которой видам самостоятельной работы может быть присвоен разный вес – от1до 4; определены критерии оценивания в тестовой форме контроля: от 30 %до 59% правильных ответов в тесте – «удовлетворительно»; 60% – 79 %– «хорошо»; 80% -100% «отлично».

Результаты своей работы вы можете отследить в личном кабинете электронно-информационной системы, к чему имеют доступ и ваши родители.

10. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ), ВКЛЮЧАЯ ПЕРЕЧЕНЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, СОВРЕМЕННЫХ ПРОФЕССИОНАЛЬНЫХ БАЗ ДАННЫХ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ

Перечень информационных технологий:

Платформа для презентаций Microsoft powerpoint;

Онлайн платформа для командной работы Miro;

Текстовый и табличный редактор Microsoft Word;

Портал института http://portal.midis.info

Перечень программного обеспечения:

1С: Предприятие. Комплект для высших и средних учебных заведений (1С – 8985755)

Mozilla Firefox

Adobe Reader
ESET Endpoint Antivirus
Microsoft™ Windows® 10 (DreamSpark Premium Electronic Software Delivery id700549166)
Microsoft™ Office®
Google Chrome
«Гарант аэро»
КонсультантПлюс
Unity
Visual Studio
XAMPP

Современные профессиональные базы данных и информационные справочные системы

«Гарант аэро»
КонсультантПлюс
Научная электронная библиотека «Elibrary.ru».

Сведения об электронно-библиотечной системе

№ п/п	Основные сведения об электронно-библиотечной системе	Краткая характеристика
1.	Наименование электронно-библиотечной системы, представляющей возможность круглосуточного дистанционного индивидуального доступа для каждого обучающегося из любой точки, в которой имеется доступ к сети Интернет, адрес в сети Интернет	Образовательная платформа «Юрайт»: https://urait.ru

11. МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

№ п/п	Наименование оборудованных учебных аудиторий, аудиторий для практических занятий	Перечень материального оснащения, оборудования и технических средств обучения
1.	**Лаборатория программного обеспечения и сопровождения компьютерных систем № 249** Лаборатория системного и прикладного программирования, технических средств обучения № 249	**Лаборатория программного обеспечения и сопровождения компьютерных систем № 249** (Лаборатория для проведения занятий всех видов, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации) *Материальное оснащение, компьютерное и интерактивное оборудование:* Компьютер Плазменная панель Компьютерный стол Стулья Стол преподавателя Стул преподавателя Автоматизированные рабочие места обеспечены доступом в электронную информационно-образовательную среду МИДиС, выходом в информационно-коммуникационную сеть «Интернет».

2.	**Библиотека. Читальный зал № 122**	**Библиотека. Читальный зал с выходом в Интернет № 122** Автоматизированные рабочие места библиотекарей Автоматизированные рабочие места для читателей Принтер Сканер Стеллажи для книг Кафедра Выставочный стеллаж Каталожный шкаф Посадочные места (столы и стулья для самостоятельной работы) Стенд информационный **Условия для лиц с ОВЗ:** Автоматизированное рабочее место для лиц с ОВЗ Линза Френеля Специальная парта для лиц с нарушениями опорно-двигательного аппарата Клавиатура с нанесением шрифта Брайля Компьютер с программным обеспечением для лиц с ОВЗ Световые маяки на дверях библиотеки Тактильные указатели направления движения Тактильные указатели выхода из помещения Контрастное выделение проемов входов и выходов из помещения Табличка с наименованием библиотеки, выполненная шрифтом Брайля Автоматизированные рабочие места обеспечены доступом в электронную информационно-образовательную среду МИДиС, выходом в информационно-коммуникационную сеть «Интернет».