МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФГБОУ ВО «Уральский государственный экономический университет»

Одобрена
на заседании кафедры

15.11.2021 г.

протокол № 4

И.о. зав. кафедрой Кислицын Е.В.

Утверждена
Советом по учебно-методическим вопросам и качеству образования

15 декабря 2021 г.

протокол № 4

Председатель _____ Карх Д.А.
(подпись)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Наименование дисциплины	Информационная безопасность и защита информации
Направление подготовки	09.03.01 Информатика и вычислительная техника
Профиль	Программное обеспечение автоматизированных систем
Форма обучения	очно-заочная
Год набора	2022

Разработана:
Доцент, к. ф.-м. н.
Зенков А.В.

Екатеринбург
2022 г.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	**3**
1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ	**3**
2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП	**3**
3. ОБЪЕМ ДИСЦИПЛИНЫ	**3**
4. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ОПОП	**3**
5. ТЕМАТИЧЕСКИЙ ПЛАН	**4**
6. ФОРМЫ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ШКАЛЫ ОЦЕНИВАНИЯ	**5**
7. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ	**7**
8. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ	**11**
9. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ УЧЕБНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ	**11**
10. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ВКЛЮЧАЯ ПЕРЕЧЕНЬ ЛИЦЕНЗИОННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ, ОНЛАЙН КУРСОВ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ	**12**
11. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ	**13**

ВВЕДЕНИЕ

Рабочая программа дисциплины является частью основной профессиональной образовательной программы высшего образования - программы бакалавриата, разработанной в соответствии с ФГОС ВО

ФГОС ВО	Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 09.03.01 Информатика и вычислительная техника (приказ Минобрнауки России от 19.09.2017 г. №
ПС	

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины «Информационная безопасность и защита информации» является формирование у студентов способности анализировать способы нарушений информационной безопасности, изучение методов защиты информационных систем, моделей безопасности и их применения. Вместе с другими предметами изучение данной дисциплины должно способствовать расширению профессионального кругозора студентов.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина относится к базовой части учебного плана.

3. ОБЪЕМ ДИСЦИПЛИНЫ

Промежуточный контроль	Часов					З.е.
	Всего за семестр	Контактная работа .(по уч.зан.)			Самостоятельная работа в том числе подготовка контрольных и курсовых	
		Всего	Лекции	Лабораторные		
Семестр 7						
Зачет	108	16	8	8	88	3

4.ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ОПОП

В результате освоения ОПОП у выпускника должны быть сформированы компетенции, установленные в соответствии ФГОС ВО.

Общепрофессиональные компетенции (ОПК)

Шифр и наименование компетенции	Индикаторы 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;	ИД-1.ОПК-3 Знать: 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 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;	ИД-2.ОПК-3 Уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
	ИД-3.ОПК-3 Иметь практический опыт:: подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности

5. ТЕМАТИЧЕСКИЙ ПЛАН

Тема	Часов						
	Наименование темы	Всего часов	Контактная работа .(по уч.зан.)			Самост. работа	Контроль самостоятельной работы
			Лекции	Лабораторные	Практические занятия		
Семестр 7		104					
Тема 1.	Международные стандарты информационного обмена. Понятие угрозы. Информационная безопасность в условиях функционирования в России глобальных сетей. Виды противников или «нарушителей». Понятия о видах	30	2	6		22	
Тема 2.	Три вида возможных нарушений информационной системы. Защита. Основные нормативные руководящие документы, касающиеся государственной тайны.	18	2			16	
Тема 3.	Нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.	12	2			10	

Тема 4.	Основные положения теории информационной безопасности информационных систем. Модели безопасности и их применение. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование.	10	2	2		6	
Тема 5.	Анализ способов нарушений информационной безопасности. Использование защищенных компьютерных систем.	10				10	
Тема 6.	Методы криптографии	12				12	
Тема 7.	Основные технологии построения защищенных информационных систем	12				12	

6. ФОРМЫ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ШКАЛЫ ОЦЕНИВАНИЯ

Раздел/Тема	Вид оценочного средства	Описание оценочного средства	Критерии оценивания
Текущий контроль (Приложение 4)			
Темы 1-3	Контрольная работа (приложение 4)	Контрольная работа содержит 1 задание	10 баллов
Тема 4-6	Контрольная работа (приложение 4)	Контрольная работа содержит 1 задание	10 баллов
Тема 7	Контрольная работа (приложение 4)	Контрольная работа содержит 1 задание	10 баллов
Промежуточный контроль (Приложение 5)			
7 семестр (За)	Билет для зачета (приложение 5)	Билет включает в себя один теоретический вопрос и одно практическое задание	100 баллов

ОПИСАНИЕ ШКАЛ ОЦЕНИВАНИЯ

Показатель оценки освоения ОПОП формируется на основе объединения текущей и промежуточной аттестации обучающегося.

Показатель рейтинга по каждой дисциплине выражается в процентах, который показывает уровень подготовки студента.

Текущая аттестация. Используется 100-балльная система оценивания. Оценка работы студента в течении семестра осуществляется преподавателем в соответствии с разработанной им системой оценки учебных достижений в процессе обучения по данной дисциплине.

В рабочих программах дисциплин и практик закреплены виды текущей аттестации, планируемые результаты контрольных мероприятий и критерии оценки учебный достижений.

В течение семестра преподавателем проводится не менее 3-х контрольных мероприятий, по оценке деятельности студента. Если посещения занятий по дисциплине включены в рейтинг, то данный показатель составляет не более 20% от максимального количества баллов по дисциплине.

Промежуточная аттестация. Используется 5-балльная система оценивания. Оценка работы студента по окончанию дисциплины (части дисциплины) осуществляется преподавателем в соответствии с разработанной им системой оценки достижений студента в процессе обучения по данной дисциплине. Промежуточная аттестация также проводится по окончанию формирования компетенций.

Порядок перевода рейтинга, предусмотренных системой оценивания, по дисциплине, в пятибалльную систему.

Высокий уровень – 100% - 70% - отлично, хорошо.

Средний уровень – 69% - 50% - удовлетворительно.

Показатель оценки	По 5-балльной системе	Характеристика показателя
100% - 85%	отлично	обладают теоретическими знаниями в полном объеме, понимают, самостоятельно умеют применять, исследовать, идентифицировать, анализировать, систематизировать, распределять по категориям, рассчитать показатели, классифицировать, разрабатывать модели, алгоритмизировать, управлять, организовать, планировать процессы исследования, осуществлять оценку результатов на высоком уровне
84% - 70%	хорошо	обладают теоретическими знаниями в полном объеме, понимают, самостоятельно умеют применять, исследовать, идентифицировать, анализировать, систематизировать, распределять по категориям, рассчитать показатели, классифицировать, разрабатывать модели, алгоритмизировать, управлять, организовать, планировать процессы исследования, осуществлять оценку результатов. Могут быть допущены недочеты, исправленные студентом самостоятельно в процессе работы (ответа и т.д.)
69% - 50%	удовлетворительно	обладают общими теоретическими знаниями, умеют применять, исследовать, идентифицировать, анализировать, систематизировать, распределять по категориям, рассчитать показатели, классифицировать, разрабатывать модели, алгоритмизировать, управлять, организовать, планировать процессы исследования, осуществлять оценку результатов на среднем уровне. Допускаются ошибки, которые студент затрудняется исправить самостоятельно.
49 % и менее	неудовлетворительно	обладают не полным объемом общих теоретическими знаниями, не умеют самостоятельно применять, исследовать, идентифицировать, анализировать, систематизировать, распределять по категориям, рассчитать показатели, классифицировать, разрабатывать модели, алгоритмизировать, управлять, организовать, планировать процессы исследования, осуществлять оценку результатов. Не сформированы умения и навыки для решения
100% - 50%	зачтено	характеристика показателя соответствует «отлично», «хорошо», «удовлетворительно»
49 % и менее	не зачтено	характеристика показателя соответствует «неудовлетворительно»

7. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

7.1. Содержание лекций

Тема 1. Международные стандарты информационного обмена. Понятие угрозы. Информационная безопасность в условиях функционирования в России глобальных сетей. Виды противников или «нарушителей». Понятия о видах вирусов.

1.1 Основные концептуальные положения системы защиты информации. Понятие информации. Структура защиты информации. Условия и требования, которым должна удовлетворять система защиты информации. Виды собственного обеспечения системы защиты информации.
1.2 Концептуальная модель информационной безопасности. Объекты угроз. Угрозы конфиденциальной информации. Конфиденциальность, полнота (целостность), достоверность и доступность информации. Ущерб от угрозы информационной безопасности.
1.3 Классификация угроз по величине принесенного ущерба, по вероятности возникновения, по причинам появления, по характеру нанесенного ущерба.
Действия, приводящие к неправомерному овладению информацией. Разглашение. Утечка. Несанкционированный доступ.

Тема 2. Три вида возможных нарушений информационной системы. Защита. Основные нормативные руководящие документы, касающиеся государственной тайны.
2.1 Правовое регулирование защиты информации. Выполнение участниками информационных правоотношений и контроль выполнения полномочными субъектами, в т.ч. правоохранительными, норм права, содержащих организационно-технические требования, дозволения и запреты в целях обеспечения целостности, доступности и конфиденциальности информации.
Интересы личности в информационной сфере. Интересы общества в информационной сфере. Интересы государства в информационной сфере.
2.2 Структура норм права Российской Федерации. Законодательства Российской Федерации в области защиты информации. Направления правого регулирования защиты информации. Конституционные гарантии интересов личности в информационной сфере.
Собственник, владелец и пользователь информационных ресурсов. Информация, не относящаяся к тайне, но распространение, которой ограничено (запрещено). Служебная или коммерческая тайна.
Руководящие документы Гостехкомиссии.
Административные правонарушения в сфере защиты информации. Составы преступлений, предусмотренные за нарушение режима защиты информации.
Электронная цифровая подпись. Закон об электронной цифровой подписи.

Тема 3. Нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.
3.1 Проблемы целостности и конфиденциальности информации на магнитных носителях.
Используемые методы защиты от непосредственного доступа к магнитным носителям.
Интеллектуальные возможности контроллера жесткого магнитного диска. Программное обеспечение для доступа и управления этими возможностями.
3.2 Физические принципы удаления и восстановления информации на магнитных носителях. Способы уничтожения информации на жестких магнитных дисках.
Обычные способы удаления файлов в файловых системах FAT, NTFS, S5/UFS. Возможности программ «шредеров». Программные и аппаратные средства уничтожения информации на HDD. Гарантированное уничтожение с разрушением магнитного носителя.
Способы восстановления информации на гибких магнитных дисках.

Тема 4. Основные положения теории информационной безопасности информационных систем. Модели безопасности и их применение. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование.
4.1 Понятие и классификация криптографических методов и средств защиты информации. Шифрование и кодирование. Ключ. Криптостойкость шифра. Характеристика некоторых методов шифрования.
4.2 Структура и классификация криптографических систем. Основные режимы работы симметричных алгоритмов и стандартов шифрования данных. Симметричные и асимметричные (с открытым ключом) криптосистемы. Алгоритмы их работы.
4.3 Аутентификация электронных документов и сообщений. Системы электронно-цифровой подписи.
4.4 Американские алгоритмы шифрования данных DES, AES, RSA.
Алгоритм шифрования данных по ГОСТ 28147-89.

7.2 Содержание практических занятий и лабораторных работ

Тема 1. Международные стандарты информационного обмена. Понятие угрозы. Информационная безопасность в условиях функционирования в России глобальных сетей. Виды противников или «нарушителей». Понятия о видах вирусов.

1. особенности современных информационных систем как объекта защиты;
2. уязвимости основных структурно-функциональных элементов компьютерных систем;
3. классификация угроз безопасности;
4. классификация каналов проникновения в информационную систему и утечки информации;
5. неформальная модель нарушителя;
6. программное обеспечение для антивирусной профилактики;
7. восстановление системной информацию, удаленных и испорченных данных;
8. основные организационные и организационно-технические мероприятия по созданию и поддержанию функционирования комплексной системы защиты;

Тема 4. Основные положения теории информационной безопасности информационных систем. Модели безопасности и их применение. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование.

1. основные меры противодействия угрозам безопасности, принципы построения систем защиты, основные механизмы защиты;
2. модели разграничения доступа;
3. криптографические методы защиты, виды средств криптозащиты данных, их достоинства и недостатки, место и роль средств криптозащиты.
4. противодействие угрозам безопасности корпоративной сети со стороны Интернет.
5. правовое регулирование защиты информации в Российской Федерации.

7.3. Содержание самостоятельной работы

Тема 1. Международные стандарты информационного обмена. Понятие угрозы. Информационная безопасность в условиях функционирования в России глобальных сетей. Виды противников или «нарушителей». Понятия о видах вирусов.

Изучение теоретического материала, основной и дополнительной литературы. Разбор лабораторных работ. Выполнение практических работ.

Тема 2. Три вида возможных нарушений информационной системы. Защита. Основные нормативные руководящие документы, касающиеся государственной тайны. Изучение теоретического материала, основной и дополнительной литературы. Разбор лабораторных работ. Выполнение практических работ.
Тема 3. Нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Изучение теоретического материала, основной и дополнительной литературы. Разбор лабораторных работ. Выполнение практических работ.
Тема 4. Основные положения теории информационной безопасности информационных систем. Модели безопасности и их применение. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование. Изучение теоретического материала, основной и дополнительной литературы. Разбор лабораторных работ. Выполнение практических работ.
Тема 5. Анализ способов нарушений информационной безопасности. Использование защищенных компьютерных систем. Изучение теоретического материала, основной и дополнительной литературы. Разбор лабораторных работ. Выполнение практических работ.
Тема 6. Методы криптографии Изучение теоретического материала, основной и дополнительной литературы. Разбор лабораторных работ. Выполнение практических работ.
Тема 7. Основные технологии построения защищенных информационных систем Изучение теоретического материала, основной и дополнительной литературы. Разбор лабораторных работ. Выполнение практических работ.

7.3.1. Примерные вопросы для самостоятельной подготовки к зачету/экзамену
Приложение 1.

7.3.2. Практические задания по дисциплине для самостоятельной подготовки к зачету/экзамену
Приложение 2.

7.3.3. Перечень курсовых работ
Не предусмотрено.

7.4. Электронное портфолио обучающегося
Материалы не размещаются.

7.5. Методические рекомендации по выполнению контрольной работы
Не предусмотрено.

7.6 Методические рекомендации по выполнению курсовой работы
Не предусмотрено.

8. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

По заявлению студента

В целях доступности освоения программы для лиц с ограниченными возможностями здоровья при необходимости кафедра обеспечивает следующие условия:

- особый порядок освоения дисциплины, с учетом состояния их здоровья;
- электронные образовательные ресурсы по дисциплине в формах, адаптированных к ограничениям их здоровья;
- изучение дисциплины по индивидуальному учебному плану (вне зависимости от формы обучения);
- электронное обучение и дистанционные образовательные технологии, которые предусматривают возможности приема-передачи информации в доступных для них формах.
- доступ (удаленный доступ), к современным профессиональным базам данных и информационным справочным системам, состав которых определен РПД.

9. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ УЧЕБНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Сайт библиотеки УрГЭУ
http://lib.usue.ru/

Основная литература:

1. Глинская Е.В., Чичварин Н.В. Информационная безопасность конструкций ЭВМ и систем [Электронный ресурс]:Учебное пособие. - Москва: ООО "Научно-издательский центр ИНФРА-М", 2021. - 118 – Режим доступа: https://znanium.com/catalog/product/1178152

2. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах [Электронный ресурс]:Учебное пособие. - Москва: Издательский Дом "ФОРУМ", 2022. - 592 – Режим доступа: https://znanium.com/catalog/product/1843022

3. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита информации [Электронный ресурс]:Учебное пособие. - Москва: Издательский Центр РИО, 2022. - 336 – Режим доступа: https://znanium.com/catalog/product/1861657

Дополнительная литература:

1. Васильков А.В., Васильков И. А. Безопасность и управление доступом в информационных системах [Электронный ресурс]:Учебное пособие. - Москва: Издательство "ФОРУМ", 2020. - 368 – Режим доступа: https://znanium.com/catalog/product/1082470

2. Партыка Т. Л., Попов И.И. Информационная безопасность [Электронный ресурс]:Учебное пособие. - Москва: Издательство "ФОРУМ", 2021. - 432 – Режим доступа: https://znanium.com/catalog/product/1189328

3. Баранова Е.К., Бабаш А.В. Информационная безопасность. История специальных методов криптографической деятельности [Электронный ресурс]:Учебное пособие. - Москва: Издательский Центр РИО, 2022. - 236 – Режим доступа: https://znanium.com/catalog/product/1843171

10. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ВКЛЮЧАЯ ПЕРЕЧЕНЬ ЛИЦЕНЗИОННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ, ОНЛАЙН КУРСОВ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Перечень лицензионного программного обеспечения:

Microsoft Windows 10 .Договор № 52/223-ПО/2020 от 13.04.2020, Акт № Tr000523459 от 14.10.2020. Срок действия лицензии 30.09.2023.

Microsoft Office 2016.Договор № 52/223-ПО/2020 от 13.04.2020, Акт № Tr000523459 от 14.10.2020 Срок действия лицензии 30.09.2023.

Перечень информационных справочных систем, ресурсов информационно-телекоммуникационной сети «Интернет»:

Справочно-правовая система Гарант. Договор № 58419 от 22 декабря 2015. Срок действия лицензии -без ограничения срока

Справочно-правовая система Консультант +. Договор № 163/223-У/2020 от 14.12.2020. Срок действия лицензии до 31.12.2021

Защита информации

https://openedu.ru/course/hse/DATPRO/

11. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Реализация учебной дисциплины осуществляется с использованием материально-технической базы УрГЭУ, обеспечивающей проведение всех видов учебных занятий и научно-исследовательской и самостоятельной работы обучающихся:

Специальные помещения представляют собой учебные аудитории для проведения всех видов занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду УрГЭУ.

Все помещения укомплектованы специализированной мебелью и оснащены мультимедийным оборудованием спецоборудованием (информационно-телекоммуникационным, иным компьютерным), доступом к информационно-поисковым, справочно-правовым системам, электронным библиотечным системам, базам данных действующего законодательства, иным информационным ресурсам служащими для представления учебной информации большой аудитории.

Для проведения занятий лекционного типа презентации и другие учебно-наглядные пособия, обеспечивающие тематические иллюстрации.