

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Силин Яков Петрович
Должность: Ректор
Дата подписания: 09.09.2021 14:45:14
Уникальный программный ключ:
24f866be2aca18484036a8cbb3c509a9531e605f

Одобрена
на заседании кафедры

26.12.2019 г.
протокол № 3
Зав. кафедрой Назаров Д.М.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФГБОУ ВО «Уральский государственный экономический университет»

Утверждена
Советом по учебно-методическим вопросам
и качеству образования

15 января 2020 г.
протокол № 5
Председатель  Карх Д.А.
(подпись)



РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Наименование дисциплины	Техническая защита информации
Направление подготовки	10.03.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
Профиль	Информационно-аналитические системы финансового мониторинга
Форма обучения	очная
Год набора	2020
Разработана:	Ассистент, Саматов К.М.
Профессор, д.э.н.	Назаров Д. М.

Екатеринбург
2020 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	6
8. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ	8
9. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ УЧЕБНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ	8
10. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ВКЛЮЧАЯ ПЕРЕЧЕНЬ ЛИЦЕНЗИОННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ, ОНЛАЙН КУРСОВ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ	9
11. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ	9

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 по направлению подготовки 10.03.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ (уровень бакалавриата) (приказ Минобрнауки России от
ПС	

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины «Техническая защита информации» является теоретическая и практическая подготовленность бакалавра к организации и проведению мероприятий по защите информации от утечки по техническим каналам на объектах информатизации и в выделенных помещениях.

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						
Экзамен	144	56	28	28	61	4

4. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ОПОП

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

Профессиональные компетенции (ПК)

Шифр и наименование компетенции	Индикаторы достижения компетенций
организационно-управленческая	
ПК-15 способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ИД-1.ПК-15 Знать: основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ России, ФСТЭК России в данной области. Уметь: пользоваться нормативными документами по защите информации; обеспечивать сохранность и неизменность обрабатываемой информации. Владеть навыками: защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.

эксплуатационная		
ПК-1 способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	ИД-1.ПК-1 Знать: типовые средства и методы защиты информации в локальных и глобальных вычислительных сетях; базовую конфигурацию системы защиты информации автоматизированной системы, особенности применения программных и программно-аппаратных средств защиты информации в автоматизированных системах; типовые средства, методы и протоколы идентификации, аутентификации и авторизации; технические средства контроля эффективности мер защиты информации; Уметь: настраивать политики безопасности наиболее распространенных операционных систем, вычислительных сетей, противодействовать нарушениям сетевой безопасности, устанавливать, настраивать и обслуживать технические и программно-аппаратные средства защиты информации. Владеть навыками по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации	
ПК-6 способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	ИД-1.ПК-6 Знать: критерии оценки эффективности программных, программно-аппаратных и технических средств защиты информации. Уметь: проводить проверку работоспособности программных, программно-аппаратных и технических средств защиты информации; проводить оценку эффективности программных, программно-аппаратных и технических средств защиты информации. Владеть способностью: принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации.	

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		18					
Тема 1.	Концепция технической защиты информации. Утечка информации по техническим каналам	18	6	2		10	
Семестр 7		38					
Тема 2.	Основные принципы технической защиты информации. Организационные основы технической защиты информации	38	8	6		24	
Семестр 7		29					
Тема 3.	Оценка угрозы утечки информации по техническим каналам и подавление опасных сигналов	29	6	10		13	
Семестр 7		32					
Тема 4.	Методы противодействия утечке и добыванию информации. Моделирование процессов технической защиты информации	32	8	10		14	

6. ФОРМЫ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ШКАЛЫ ОЦЕНИВАНИЯ

Раздел/Тема	Вид оценочного средства	Описание оценочного средства	Критерии оценивания
Текущий контроль (Приложение 4)			
Тема 1	Тест №1 (Приложение 4)	Тест состоит из 10 вопросов	<30 - не зачет 31<...<65 - 3 66<...<80 - 4 81<...<100 - 5
Тема 2	Доклад, сообщение (Приложение 4)	Продукт самостоятельной работы студента, представляющий собой публичное выступление по представлению полученных результатов решения определенной учебно-практической, учебно-исследовательской и научной темы.	<30 - не зачет 31<...<65 - 3 66<...<80 - 4 81<...<100 - 5
Тема 3	Контрольная работа № 1 (Приложение 4)	Контрольная работа состоит из 2 заданий по вариантам	<30 - не зачет 31<...<65 - 3 66<...<80 - 4 81<...<100 - 5
Тема 4	Контрольная работа № 2 (Приложение 4)	Контрольная работа состоит из 2 заданий по вариантам	<30 - не зачет 31<...<65 - 3 66<...<80 - 4 81<...<100 - 5
Промежуточный контроль (Приложение 5)			
7 семестр (Эк)	Экзаменационный билет (Приложение 5)	В билете 2 теоретических и 1 практический вопрос	<30 - не зачет 31<...<65 - 3 66<...<80 - 4 81<...<100 - 5

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 учебных 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. Концепция технической защиты информации. Утечка информации по техническим каналам

Тема 2. Основные принципы технической защиты информации. Организационные основы технической защиты информации Основные принципы технической защиты информации.
Тема 3. Оценка угрозы утечки информации по техническим каналам и подавление опасных сигналов Оценка угрозы утечки информации по техническим каналам и подавление опасных сигналов
Тема 4. Методы противодействия утечке и добыванию информации. Моделирование процессов технической защиты информации Методы противодействия утечке и добыванию информации. Моделирование процессов технической защиты информации

7.2 Содержание практических занятий и лабораторных работ

Тема 1. Концепция технической защиты информации. Утечка информации по техническим каналам Изучение способов защиты информации от утечки по техническим каналам
Тема 2. Основные принципы технической защиты информации. Организационные основы технической защиты информации Организационные основы технической защиты информации
Тема 3. Оценка угрозы утечки информации по техническим каналам и подавление опасных сигналов Оценка угрозы утечки информации по техническим каналам и подавление опасных сигналов
Тема 4. Методы противодействия утечке и добыванию информации. Моделирование процессов технической защиты информации Моделирование защиты информации от утечки по техническим каналам

7.3. Содержание самостоятельной работы

Тема 1. Концепция технической защиты информации. Утечка информации по техническим каналам Изучение концепции технической защиты информации, способов утечки информации по техническим каналам
Тема 2. Основные принципы технической защиты информации. Организационные основы технической защиты информации Основные принципы технической защиты информации. Организационные основы технической защиты информации
Тема 3. Оценка угрозы утечки информации по техническим каналам и подавление опасных сигналов Оценка угрозы утечки информации по техническим каналам и подавление опасных сигналов
Тема 4. Методы противодействия утечке и добыванию информации. Моделирование процессов технической защиты информации Методы противодействия утечке и добыванию информации. Моделирование процессов технической защиты информации

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
Курсовые работы не предусмотрены

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. Баранова Е.К., Бабаш А.В.. Информационная безопасность и защита информации [Электронный ресурс]: Учебное пособие. - Москва: Издательский Центр РИОР, 2016. - 322 с. – Режим доступа: <https://new.znaniium.com/catalog/product/495249>

1. Анисимов А. Л.. Правовые аспекты информационной безопасности. Ч. 2 [Электронный ресурс]: учебное пособие. - Екатеринбург: [Издательство УрГЭУ], 2016. - 87 с. – Режим доступа: <http://lib.usue.ru/resource/limit/ump/16/p486180.pdf>

2. Васильков А.В., Васильков И. А.. Безопасность и управление доступом в информационных системах [Электронный ресурс]: Учебное пособие. - Москва: Издательство "ФОРУМ", 2017. - 368 с. – Режим доступа: <https://new.znaniium.com/catalog/product/537054>

3. Баранова Е.К., Бабаш А.В.. Моделирование системы защиты информации: Практикум [Электронный ресурс]: Учебное пособие. - Москва: Издательский Центр РИОР, 2016. - 224 с. – Режим доступа: <https://new.znaniium.com/catalog/product/549914>

Дополнительная литература:

1. Максимов Н. В., Партыка Т. Л.. Технические средства информатизации [Электронный ресурс]: Учебник. - Москва: Издательство "ФОРУМ", 2010. - 592 с. – Режим доступа: <https://new.znaniium.com/catalog/product/214957>

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

Перечень лицензионное программное обеспечение:

СЗИ от НСД "Страж NT" версия 4.0. Договор № 73700092 от 04.08.2017, Товарная накладная № 73700092 от 11.10.2017.

Secret Net 7. Клиент (автономный режим работы). Договор № 73700092 от 04.08.2017, Товарная накладная № 73700092 от 11.10.2017.

Позитив Текнолоджиз MaxPatrol 8.

Позитив Текнолоджиз Xspider.

Astra Linux Common Edition. Договор № 1 от 13 июня 2018, акт от 17 декабря 2018. Срок действия лицензии - без ограничения срока.

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 № 194-У-2019 от 09.01.2020. Срок действия лицензии до 31.12.2020

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.