

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Силин Яков Петрович
Должность: Ректор
Дата подписания: 31.08.2023 11:55:23
Уникальный программный идентификатор:
24f866be2aca16484036a8cbb3c509e9531b605f

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

05.12.2022 г.
протокол № 4
Зав. кафедрой Назаров Д.М.

Утверждена
Советом по учебно-методическим
вопросам и качеству образования
14 декабря 2022 г.
протокол № 4
Председатель (подпись) Карх Д.А.



РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Наименование дисциплины Защита информации в банковских информационных системах
Направление подготовки 10.03.01 Информационная безопасность
Профиль Информационно-аналитические системы финансового мониторинга

Форма обучения очная
Год набора 2023

Разработана:
Доцент, к.э.н.
Буценко Е.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	5
6. ФОРМЫ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ШКАЛЫ ОЦЕНИВАНИЯ	6
7. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ	8
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	12

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 10.03.01 Информационная безопасность (приказ Минобрнауки России от 17.11.2020 г. № 1427)
ПС	

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины является формирование у студентов компетенций, направленных на изучение теоретических основ и практическое освоение методики обеспечения защиты информации в банковских системах и в кредитно-финансовой сфере России.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина относится к вариативной части учебного плана.

3. ОБЪЕМ ДИСЦИПЛИНЫ

Промежуточный контроль	Часов					3.е.
	Всего за семестр	Контактная работа (по уч.зан.)			Самостоятельная работа в том числе подготовка контрольных и курсовых	
		Всего	Лекции	Лабораторные		
Семестр 6						
Экзамен	180	108	36	72	36	5

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
эксплуатационный	

<p>ПК-3 Подготовка данных для проведения аналитических работ по исследованию больших данных</p>	<p>ИД-1.ПК-3 Знать:</p> <p>Архитектура подсистем защиты информации в операционных системах</p> <p>Принципы построения систем управления базами данных</p> <p>Основные средства и методы анализа программных реализаций</p> <p>Принципы построения антивирусного программного обеспечения</p> <p>Виды политик управления доступом и информационными потоками применительно к прикладному программному обеспечению</p> <p>Источники угроз информационной безопасности программного обеспечения и меры по их предотвращению</p> <p>Уязвимости используемого программного обеспечения и методы их эксплуатации</p> <p>Виды и формы функционирования вредоносного программного обеспечения</p> <p>Характерные признаки наличия вредоносного программного обеспечения</p> <p>Средства и методы обнаружения ранее неизвестного вредоносного программного обеспечения</p> <p>Принципы функционирования программных средств криптографической защиты информации</p> <p>Порядок обеспечения безопасности информации при эксплуатации программного обеспечения</p> <p>Нормативные правовые акты в области защиты информации</p> <p>Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации</p> <p>Организационные меры по защите информации</p>
	<p>ИД-2.ПК-3 Уметь:</p> <p>Анализировать угрозы безопасности информации программного обеспечения</p> <p>Формулировать правила безопасной эксплуатации программного обеспечения</p> <p>Обосновывать правила безопасной эксплуатации программного обеспечения</p> <p>Анализировать функционирование программного обеспечения с целью определения возможного вредоносного воздействия</p> <p>Производить проверку соответствия реальных характеристик программно-аппаратных средств защиты информации заявленным в их технической документации</p> <p>Осуществлять мероприятия по противодействию угрозам безопасности информации, возникающим при эксплуатации программного обеспечения</p> <p>Определять порядок функционирования программного обеспечения с целью обеспечения защиты информации</p> <p>Анализировать эффективность сформулированных требований к встроенным средствам защиты информации программного обеспечения</p>

<p>ПК-3 Подготовка данных для проведения аналитических работ по исследованию больших данных</p>	<p>ИД-3.ПК-3 Иметь практический опыт: Определение порядка установки программного обеспечения с целью соблюдения требований по защите информации Контроль над соблюдением требований по защите информации при установке программного обеспечения, включая антивирусное программное обеспечение Формулирование требований к параметрам средств антивирусной защиты для корректной работы программного обеспечения Выполнение работ по обнаружению вредоносного программного обеспечения Ликвидация обнаруженного вредоносного программного обеспечения и последствий его функционирования Формулирование требований к встроенным средствам защиты информации программного обеспечения</p>
---	---

5. ТЕМАТИЧЕСКИЙ ПЛАН

Тема	Часов						
	Наименование темы	Всего часов	Контактная работа (по уч.зан.)			Самост. работа	Контроль самостоятельной работы
			Лекции	Лабораторные	Практические занятия		
Семестр 6		20					
Тема 1.	Требования к информационной безопасности банка	20	6	4		10	
Семестр 6		20					
Тема 2.	Общие принципы защиты информации в банковских информационных системах	20	6	4		10	
Семестр 6		18					
Тема 3.	Автоматизация банковских операций и их защита	18	6	12			
Семестр 6		26					
Тема 4.	Методы защиты информации в автоматизированных системах обработки данных. Криптографические технологии защиты информации. ЭЦП. Полиграфические и голографические методы защиты от фальсификации документов и ценных бумаг	26	6	20			
Семестр 6		20					
Тема 5.	Автоматизация валютных операций	20	6	4		10	
Семестр 6		22					
Тема 6.	Защита информации при выполнении электронных платежей	22	6	16			
Семестр 6		18					
Тема 7.	Реализация технологий цифровой подписи, цифрового конверта, цифрового сейфа	18		12		6	

6. ФОРМЫ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ШКАЛЫ ОЦЕНИВАНИЯ

Раздел/Тема	Вид оценочного средства	Описание оценочного средства	Критерии оценивания
Текущий контроль (Приложение 4)			
3. Автоматизация банковских операций и их защита. Угрозы безопасности автоматизированных банковских систем. Особенности защиты информации в электронных банковских системах	Тест (Приложение 4)	Тест состоит из 30 вопросов с вариантами ответов	1-10 баллов
2. Общие принципы защиты информации в банковских информационных системах	Тест (Приложение 4)	Тест состоит из 30 вопросов с вариантами ответов	1-10 баллов
1. Требования к информационной безопасности банка	Тест (Приложение 4)	Тест состоит из 30 вопросов с вариантами ответов	1-10 баллов
Промежуточный контроль (Приложение 5)			
6 семестр (Эк)	Экзаменационный билет (приложение 5)	27 билетов. 2 теоретических вопроса и 1 практическое задание	1-100 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 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 профессиональных задач
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

<p>Тема 1. Требования к информационной безопасности банка Роли и обязанности должностных лиц по проведению политики безопасности. Аудит информационной безопасности. Нормы и стандарты информационной безопасности на предприятии</p>
<p>Тема 2. Общие принципы защиты информации в банковских информационных системах Защита банковской информации. Несанкционированный доступ. Федеральный закон о деятельности банков. Защита от физического доступа. Защита резервных копий. Защита от инсайдеров</p>
<p>Тема 3. Автоматизация банковских операций и их защита Автоматизация банковских операций и их защита. Необходимость защиты банковских систем: тенденции и факты. Угрозы безопасности автоматизированных банковских систем. Особенности защиты информации в электронных банковских системах</p>
<p>Тема 4. Методы защиты информации в автоматизированных системах обработки данных. Криптографические технологии защиты информации. ЭЦП. Полиграфические и голографические методы защиты от фальсификации документов и ценных бумаг ЭЦП. Криптография. Голография. Принцип голографии. Полиграфические средства защиты</p>
<p>Тема 5. Автоматизация валютных операций Нормативная база защиты информации в финансово-кредитной сфере. Принципы политики безопасности</p>
<p>Тема 6. Защита информации при выполнении электронных платежей Понятие электронной платежной системы. Безопасность в электронных платежных системах. Электронные пластиковые карты</p>

7.2 Содержание практических занятий и лабораторных работ

<p>Тема 1. Требования к информационной безопасности банка Методология защиты автоматизированных систем обработки информации. Безопасность АСОИ</p>
<p>Тема 2. Общие принципы защиты информации в банковских информационных системах Объекты защиты коммерческого банка. Государственные акты и стандарты защиты информации. Функции системы имитационного моделирования по управлению предприятием в условиях рыночной экономики</p>
<p>Тема 3. Автоматизация банковских операций и их защита</p> <ol style="list-style-type: none"> 1. Банковские операции и их защита 2. Объекты и назначение средств программной защиты

Тема 4. Методы защиты информации в автоматизированных системах обработки данных. Криптографические технологии защиты информации. ЭЦП. Полиграфические и голографические методы защиты от фальсификации документов и ценных бумаг

1. Подпись документов при помощи симметричных криптосистем
2. Хэш-функция
3. Хранение ключей
4. Распределение ключей
5. Стандарты криптографии
6. Требования пользователей
7. Атаки на цифровую подпись
8. Атаки на алгоритмы
9. Атаки на криптосистему
10. Атаки на реализацию
11. Атаки на пользователей
12. Электронные цифровые подписи
13. Алгоритмы электронной цифровой подписи
14. "КриптоБанк"
15. Юридические аспекты использования технологии для контроля подлинности документов

Тема 5. Автоматизация валютных операций

Нормативные акты Банка России

Тема 6. Защита информации при выполнении электронных платежей

1. Кодирование магнитной полосы пластиковой карты
2. Программирование микросхемы

Тема 7. Реализация технологий цифровой подписи, цифрового конверта, цифрового сейфа

1. Цифровая подпись "Нотариус".
2. Цифровой конверт "Веста".
3. Криптосейф

7.3. Содержание самостоятельной работы

Тема 1. Требования к информационной безопасности банка

Изучение понятийного аппарата темы, методического материала, глав рекомендованных учебников и дополнительных источников

Тема 2. Общие принципы защиты информации в банковских информационных системах

Изучение понятийного аппарата темы, методического материала, глав рекомендованных учебников и дополнительных источников

Тема 5. Автоматизация валютных операций

Изучение понятийного аппарата темы, методического материала, глав рекомендованных учебников и дополнительных источников

Тема 7. Реализация технологий цифровой подписи, цифрового конверта, цифрового сейфа

Изучение понятийного аппарата темы, методического материала, глав рекомендованных учебников и дополнительных источников

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
Материалы не предусмотрены

7.6 Методические рекомендации по выполнению курсовой работы
Материалы не предусмотрены

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. Финансовый университет при Правительстве Российской Федерации Кибербезопасность в условиях электронного банкинга [Электронный ресурс]: Практическое пособие. - Москва: Прометей, 2020. - 522 с. – Режим доступа: <https://znanium.com/catalog/product/1284190>

2. Внуков А. А. Защита информации в банковских системах [Электронный ресурс]: учебное пособие для вузов. - Москва: Юрайт, 2022. - 246 с – Режим доступа: <https://urait.ru/bcode/490278>

Дополнительная литература:

1. Полякова Т. А., Стрельцов А. А., Чубукова С. Г., Ниесов В. А. Организационное и правовое обеспечение информационной безопасности [Электронный ресурс]: учебник и практикум для вузов. - Москва: Юрайт, 2022. - 325 с – Режим доступа: <https://urait.ru/bcode/498844>

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:

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

Libre Office. Лицензия GNU LGPL. Срок действия лицензии - без ограничения срока.

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.

Microsoft Visual Studio Community. Лицензия для образовательных учреждений. Срок действия лицензии - без ограничения срока.

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

Справочно-правовая система Консультант +. Срок действия лицензии до 31.12.2023

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

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.