



Федеральное государственное бюджетное образовательное учреждение высшего образования
«ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ ДВАЖДЫ ГЕРОЯ
СОВЕТСКОГО СОЮЗА, ЛЕТЧИКА-КОСМОНАВТА А.А. ЛЕОНОВА»

«УТВЕРЖДАЮ»

И.о. проректора

А.В. Троицкий

«__» _____ 2023 г.

**ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И
ТЕХНОЛОГИЙ**

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**РАБОЧАЯ ПРОГРАММА
ДИСЦИПЛИНЫ (МОДУЛЯ)**

**Б.1.В.ДВ.03.02 «ЗАЩИЩЕННЫЕ ЭЛЕКТРОННЫЕ
ТЕХНОЛОГИИ БАНКА»**

Направление подготовки: 10.03.01 Информационная безопасность

Профиль: Организация и технологии защиты информации

Уровень высшего образования: бакалавриат

Форма обучения: очная, очно-заочная

Королев
2023

Рабочая программа является составной частью основной профессиональной образовательной программы и проходит рецензирование со стороны работодателей в составе основной профессиональной образовательной программы. Рабочая программа актуализируется и корректируется ежегодно.

Автор: Сухотерин А.И. Рабочая программа дисциплины: «Защищенные электронные технологии банка». – Королев МО: «Технологический университет», 2023.

Рецензент: Соляной В.Н.

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки бакалавров 10.03.01 «Информационная безопасность» и Учебного плана, утвержденного Ученым советом Университета. Протокол № 9 от 11.04.2023 года.

Рабочая программа рассмотрена и одобрена на заседании кафедры:

Заведующий кафедрой (ФИО, ученая степень, звание, подпись)	• к.в.н., доцент Соляной В.Н.			
Год утверждения (переутверждения)	2023	2024	2025	2026
Номер и дата протокола заседания кафедры	118 от 29.03.2023			

Рабочая программа согласована:

Руководитель ОПОП ВО

 к.в.н., доцент Сухотерин А.И.

Рабочая программа рекомендована на заседании УМС:

Год утверждения (переутверждения)	2023	2024	2025	2026
Номер и дата протокола заседания УМС	115 от 11.04.2023			

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ОПОП ВО

Целью изучения дисциплины является:

1. Ускоренная адаптация студентов в предметную область информационная безопасность, опираясь на весь спектр научных воззрений, на развитие и защиту информационно - телекоммуникационной инфраструктуры и компьютерной информации в кредитно – финансовой сфере;
2. Повысить уровень специальных знаний, которые необходимы обучающимся для высоко профессиональной деятельности во всех сферах информационной безопасности с учетом требований высшей школы, для активизации их учебной и исследовательской деятельности;
3. Формирование у студентов специализированной базы знаний по основным понятиям в области информационной безопасности банковской деятельности;
4. Приобретение студентами первичных навыков по практическому формированию комплекса документов, составляющих правовую базу защиты информации в банковской сфере.

В процессе обучения студент приобретает и совершенствует следующие компетенции.

ПК-1. Способность проводить исследования защищенности информационных объектов на соответствие требованиям нормативно-правовых актов и стандартов в области информационной безопасности

ПК-2. Способность принимать участие в проведении экспериментальных исследований системы защиты информации.

Основными задачами дисциплины являются:

1. Ознакомить студентов с задачами в области безопасности банковской деятельности на основе действующего российского законодательства;
2. Научить студентов самостоятельно решать поставленные задачи в области защиты информации в банках по базовым направлениям защиты банковской тайны и конфиденциальной информации;
3. Формировать систему знаний у обучающихся в области защиты информации в кредитно финансовой сфере деятельности.

4. Изучить основы организации противодействия угрозам информационной безопасности в кредитно – финансовой сфере;
5. Ознакомить с системным описанием внешних угроз безопасности кредитно – финансовой деятельности, правовых и организационных основ противодействия им, а также техники обеспечения безопасности кредитно – финансовой организации;
6. Ознакомить с методами и средствами защиты информации банковских инструментов и технологий функциональных и контролирующих подразделений финансово – кредитных организаций.

Показатель освоения компетенции отражают следующие индикаторы:

Необходимые знания:

- нормативно-правовые акты и стандарты в области ИБ и принципы проведения диагностики системы ЗИ;
- руководящие и методические документы принципы организации по проведению экспериментальной деятельности в области ЗИ;

Необходимые умения:

- выявлять и оценивать источники и последствия инцидентов ИБ (ЗИ);
- применять действующую нормативную базу выбирать целесообразные потребные средства и определять структуру системы ЗИ в ходе проведения экспериментов;

Трудовые действия:

- выполнять обнаружение, идентификацию и устранение инцидентов ИБ (ЗИ);
- разрабатывать модели, проекты и предложения в ходе проведения экспериментов деятельности по совершенствованию системы ЗИ;

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Защищенные электронные технологии банка» относится к дисциплинам по выбору вариативной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность», профиль: «Организация и технологии защиты информации».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Информатика», «Основы права», «Основы управленческой деятельности» и компетенциях: ОПК-1,6,7,8,9,13; УК-5,6,9.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Организация

защиты персональных данных на предприятии», «Правовая охрана результатов интеллектуальной деятельности», «Организация системы обеспечения информационной безопасности (служба ИБ)», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

3. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины для студентов очной и очно-заочной формы составляет 3 зачетных единицы, 108 часов.

Таблица 1

Виды занятий	Всего часов	Семестр 6	Семестр 7	Семестр ...	Семестр ...
Общая трудоемкость	108	108	108		
ОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	32	32			
Лекции (Л)	16	16			
Практические занятия (ПЗ)	16	16			
Лабораторные работы (ЛР)	-	-			
Самостоятельная работа	66	66			
Другие виды контактной работы	10	10			
Практическая подготовка	8	8			
Курсовые работы (проекты)	-	-			
Расчетно-графические работы	-	-			
Контрольная работа, домашнее задание	+	+			
Текущий контроль знаний (7 - 8, 15 - 16 недели) – 2ч	T1;T2	T1;T2			
Вид итогового контроля	Экзамен	Экзамен			
ОЧНО-ЗАОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	28		28		
Лекции (Л)	12		12		
Практические занятия (ПЗ)	16		16		
Лабораторные работы (ЛР)	-		-		
Другие виды контактной работы	10		10		
Самостоятельная работа	78		78		
Курсовые работы (проекты)	-		-		

Расчетно-графические работы	-		-		
Контрольная работа, домашнее задание	+		+		
Практическая подготовка	нет		нет		
Вид итогового контроля	Экзамен		Экзамен		

Под другими видами контактной работы понимается: групповые и индивидуальные консультации, тестирование

4. Содержание дисциплины

4.1. Темы дисциплины и виды занятий

Таблица 2

Наименование тем	Лекции, час. Очно е/очно- заочное	Практические занятия, час Очное/очно-заочное	Занятия в интерактивной форме, час	Практическая подготовка, час	Код компетенций
Раздел I. Основы информационной безопасности банковской деятельности					
Тема 1. Концептуальные основы информационной безопасности банка	1/0,5	1/1	1/1	1/-	ПК-1
Тема 2. Правовые основы информационной безопасности банка	1/0,5	1/1	1/1	0.5/-	ПК-1
Тема 3. Стандарты информационной безопасности банка	1/0,5	1/1	1/1	0.5/-	ПК-1
Тема 4. Организационные основы информационной безопасности банка	1/0,5	1/1	1/1	0.5/-	ПК-1
Тема 5. Техника обеспечения	2/1	2/2	1/1	0.5/-	ПК-1

информационно й безопасности банка					
Тема 6. Защита от информационны х преступлений, посягающих на собственность банка	2/1	2/2	2/1	1/-	ПК-2
Раздел II. Технологии защиты информации в банковской деятельности					
Тема 7. Защита от хищения денежных средств и иного имущества с использованием векселей (информационн ый аспект)	2/2	2/2	2/1	1/-	ПК-2
Тема 8. Защита от информационн ых преступлений, посягающих на информационну ю безопасность функционирова ния банка	2/2	2/2	1/1	1/-	ПК-2
Тема 9. Организация противодействи я отмыванию преступных доходов и финансировани ю терроризма (информационн ый аспект)	2/2	2/2	1/1	1/-	ПК-2
Тема 10. Комплексное обеспечение информационно й безопасности банка	2/2	2/2	1/1	1/-	ПК-2
Итого:	16/12	16/16	12/10	8/нет	

4.2. Содержание тем дисциплины

Раздел I. Основы информационной безопасности банковской деятельности

Тема 1. Концептуальные основы безопасности банка

Понятия и концепция безопасности банка. Банк как объект противоправных посягательств. Система угроз безопасности банка. Банк как субъект борьбы с противоправными посягательствами.

Тема 2. Правовые основы информационной безопасности банка

Система правового обеспечения безопасности банка. Правовые акты общего действия, обеспечивающие безопасность банков методами охранительного содержания. Банковское законодательство. Нормативные акты Банка России. Внутренние нормативные акты. Содержание аудита по ИБ технических средств обработки информации.

Тема 3. Стандарты информационной безопасности банка

О Стандарте Банка России “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения.

Основные цели и задачи стандарта Банка России при обеспечении информационной безопасности.

Основные направления работы по дальнейшему сопровождению и доработке Стандарта в рамках специально созданного Подкомитетом 3 “Защита информации в кредитно-финансовой сфере” Технического комитета 362 “Защита информации” Федерального агентства по техническому регулированию и метрологии.

Аудит информационной безопасности банка.

Преимущества и недостатки выполнения работ по защите ПДн в рамках Стандарт Банка России СТО БР ИББС 1.0-2006.

Система технических средств безопасности банка. Технические средства охраны. Технические средства охраны банковских операций и продуктов. Техничко – криминалистические средства.

Тема 4. Организационные основы информационной безопасности банка

Организация системы безопасности банка. Субъекты обеспечения безопасности банка. Средства и методы обеспечения безопасности банка. Организация внутреннего контроля банка. Организация службы безопасности банка.

Тема 5. Техника обеспечения информационной безопасности банка

Система технических средств безопасности банка. Технические средства охраны. Технические средства охраны банковских операций и продуктов. Техничко – криминалистические средства.

Тема 6. Защита от информационных преступлений, посягающих на собственность банка

Хищения денежных средств, при совершении кредитных операций. Хищения денежных средств с незаконным использованием пластиковых

карт. Хищения денежных средств с использованием аккредитивов. Хищение денежных средств с использованием чеков. Хищение денежных средств с использованием платежных поручений.

Раздел II. Технологии защиты информации в банковской деятельности

Тема 7. Защита от хищения денежных средств и иного имущества с использованием векселей (информационный аспект)

Правовая характеристика векселя. Риски в сфере вексельного обращения. Преступления против собственности, в которых вексель является предметом посягательств. Преступления против собственности, в которых вексель является средством совершения преступления. Меры предупреждения преступлений в сфере вексельного обращения.

Тема 8. Защита от информационных преступлений, посягающих на информационную безопасность функционирования банка

Злоупотребления полномочиями. Коммерческий подкуп. Противоправные посягательства на сведения банка, составляющие банковскую, коммерческую и служебную тайну. Противоправные посягательства в сфере компьютерного обеспечения деятельности банка. Противоправные посягательства на кадровое обеспечение банка. Противоправные посягательства на нематериальные активы банка.

Тема 9. Организация противодействия отмыванию преступных доходов и финансированию терроризма (информационный аспект)

Понятие и правовая характеристика легализации (отмывания) доходов, полученных преступным путем. Криминалистическая характеристика легализации и отмывания преступных доходов. Система мер предупреждения легализации (отмывания) доходов, полученных преступным путем, и финансирования терроризма.

Тема 10. Комплексное обеспечение информационной безопасности банка

Информация, используемая в целях обеспечения безопасности банка, и ее источники. Бюро кредитных историй. Специальные аналитические технологии для предупреждения и расследования противоправных посягательств на безопасность банка

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

«Методические указания для самостоятельной работы обучающихся по освоению дисциплины» представлены в Приложении 2.

6. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

Структура фонда оценочных средств, для проведения промежуточной аттестации обучающихся по дисциплине «Защищенные электронные технологии банка» приведена в Приложении 1.

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

Основная литература:

1. Кибербезопасность в условиях электронного банкинга : практическое пособие / под ред. П. В. Ревенкова. - Москва : Прометей, 2020. - 522 с. - ISBN 978-5-907244-61-0. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1284190> (дата обращения: 28.11.2022). – Режим доступа: по подписке.
2. Бабаш, А. В. Моделирование системы защиты информации. Практикум : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 3-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 320 с. + Доп. материалы [Электронный ресурс]. — (Высшее образование). — DOI: <https://doi.org/10.29039/01848-4>. - ISBN 978-5-369-01848-4. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1232287> (дата обращения: 28.11.2022). – Режим доступа: по подписке.

Дополнительная литература:

3. Тавасиев, А. М. Банковское кредитование : учебник / А.М. Тавасиев, Т.Ю. Мазурина, В.П. Бычков ; под ред. А.М. Тавасиева. — 2-е изд., перераб. — Москва : ИНФРА-М, 2020. — 366 с. — (Среднее профессиональное образование). - ISBN 978-5-16-014239-5. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1039295> (дата обращения: 28.11.2022). – Режим доступа: по подписке.

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

Интернет-ресурсы:

1. <http://eup.ru/catalog/all-all.asp> – научно-образовательный портал.
2. <http://informika.ru/> – образовательный портал.
3. www.wikIsec.ru - Энциклопедия информационной безопасности. – Публикации, статьи.
4. www.biblioclub.ru - Универсальная библиотека онлайн.
5. www.rucont.ru - ЭБС «Руконт».
6. <http://www.academy.it.ru/> – академия АЙТИ.

7. <http://www.minfin.ru> - Официальный сайт Министерства финансов Российской Федерации
8. <http://www.gov.ru/> - Официальный сервер органов государственной власти Российской Федерации.
9. <http://www.fsb.ru/> - Официальный сайт Федеральной Службы Безопасности
10. <http://www.fstec.ru/> - Официальный сайт Федеральной Службы по Техническому Экспортному контролю

9. Методические указания для обучающихся, по освоению дисциплины

Методические указания для обучающихся, по освоению дисциплины приведены в Приложении 2 к настоящей рабочей программе.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

Перечень программного обеспечения: MSOffice, PowerPoint.

Информационные справочные системы:

1. Электронные ресурсы образовательной среды Университета.
2. Информационно-справочные системы (Консультант+; Гарант).

Ресурсы информационно-образовательной среды Университета:

Рабочая программа и методическое обеспечение по курсу «Защищенные электронные технологии банка».

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

Лекционные занятия:

- аудитория, оснащенная презентационной техникой (проектор, экран);
- комплект электронных презентаций / слайдов на темы:

Практические занятия:

- компьютерный класс с проектором для интерактивного обучения и проведения лекций в форме слайд-презентаций, оборудованный современными лицензионными программно-техническими средствами: операционная система не ниже WindowsXP; офисные программы MSOffice 7;

- рабочее место преподавателя, оснащенное компьютером с доступом в Интернет;
- рабочие места студентов, оснащенные компьютерами с доступом в Интернет.

**Фонд оценочных средств для проведения промежуточной аттестации
обучающихся по дисциплине (модулю)**

**ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И
ТЕХНОЛОГИЙ**

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ
ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО
ДИСЦИПЛИНЕ**

«ЗАЩИЩЕННЫЕ ЭЛЕКТРОННЫЕ ТЕХНОЛОГИИ БАНКА»

Направление подготовки: 10.03.01 «Информационная безопасность»

Профиль: Организация и технологии защиты информации

Уровень высшего образования: бакалавриат

Форма обучения: очная, очно-заочная

Королев
2023

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

№ п/п	Индекс компетенции	Содержание компетенции	Раздел дисциплины, обеспечивающий формирование компетенции	В результате изучения раздела дисциплины, обеспечивающего формирование компетенции, обучающийся приобретает:		
				Трудовые действия	Необходимые умения	Необходимые знания
1.	ПК-1	Способность проводить исследования защищенности информационных объектов на соответствие требованиям нормативно-правовых актов и стандартов в области информационной безопасности	Тема:1-5	- выполнять обнаружение, идентификацию и устранение инцидентов ИБ (ЗИ);	- выявлять и оценивать источники и последствия инцидентов ИБ (ЗИ);	- нормативно-правовые акты и стандарты в области ИБ и принципы проведения диагностики системы ЗИ;
2.	ПК-2	Способность принимать участие в проведении экспериментальных исследований системы защиты информации	Тема:6-10	- разрабатывать модели, проекты и предложения в ходе проведения экспериментов и по совершенствованию системы ЗИ;	- применять действующую нормативную базу выбирать целесообразные средства и определять структуру системы ЗИ в ходе проведения экспериментов;	- руководящие и методические документы принципы организации по проведению экспериментальной деятельности в области ЗИ;

2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Код компетенции	Инструмент, оценивающий сформированность компетенции	Этапы и показатель оценивания компетенции	Критерии оценивания компетенции на различных этапах формирования и шкалы оценивания
ПК-1,2	Доклад	<p>А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 5 баллов</p> <p>Б) частично сформирована:</p> <ul style="list-style-type: none"> • компетенция освоена на <u>продвинутом</u> уровне – 4 балла; • компетенция освоена на <u>базовом</u> уровне – 3 балла; <p>В) не сформирована (компетенция <u>не сформирована</u>) – 2 и менее баллов</p>	<p>Например: Проводится в письменной и/или устной форме. Критерии оценки:</p> <ol style="list-style-type: none"> 1. Соответствие содержания доклада заявленной тематике (1 балл). 2. Качество источников и их количество при подготовке работы (1 балл). 3. Владение информацией и способность отвечать на вопросы аудитории (1 балл). 4. Качество самой представленной работы (1 балл). 5. Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл). <p>Максимальная сумма баллов - 5 баллов.</p>
ПК-1,2	Выполнение контрольной работы	<p>А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 5 баллов</p> <p>Б) частично</p>	<p>При определении сформированности компетенций критериями оценивания выступают методические</p>

		<p>сформирована:</p> <ul style="list-style-type: none"> • компетенция освоена на <u>продвинутом</u> уровне – 4 балла; • компетенция освоена на <u>базовом</u> уровне – 3 балла; <p>В) не сформирована (<u>компетенция не сформирована</u>) – 2 и менее баллов</p>	<p>рекомендации, разработанные по дисциплине для данного вида</p>
--	--	---	--

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

Примерная тематика докладов в презентационной форме:

1. Информационные технологии управления КБ и иные технологии оказания КБ услуги роль информационной безопасности при их применении.
2. Состав и свойства информационных объектов СБ (системы бюджетирования). Функциональность и алгоритмы СБ и ее информационная безопасность.
3. Информационная безопасность при оказании услуги и выполнении операций в кредитном учреждении.
4. Органические структуры. Управленческие функции и их разделение в банке. Информационное взаимодействие управленческой и аналитической служб. Организационная структура КБ. Подсистема ядра БИС. Роль и место службы информационной безопасности
5. Информационная безопасность подсистемы ведения индивидуальных счетов клиентов.
6. Информационная безопасность подсистемы работы с банковскими картами.
7. Информационная безопасность подсистемы кредитования и подсистема валютно – обменных операций.
8. Информационная безопасность подсистема операций с ценными бумагами.
9. Информационная безопасность подсистема инкассации и подсистемы межбанковского взаимодействия.

10. Информационная безопасность подсистемы управления ресурсами (диллинга).

11. Информационная безопасность в подсистеме обеспечения безопасности.

12. Информационная безопасность подсистемы генерации отчетов, планирования и анализа деятельности.

13. Информационная безопасность подсистема удаленного банковского обслуживания.

14. Информационная безопасность подсистема обеспечения внутренней деятельности банка как субъекта экономики.

15. Информационная безопасность системы электронного документооборота банка.

16. Информационная безопасность традиционных технологий расчетов.

17. Информационная безопасность и архитектура системы «Клиент – банк».

18. Информационная безопасность и способы передачи информации до компьютерной сети банка.

19. Информационная безопасность системы телефонного банкинга.

20. Информационная безопасность системы «Клиент – банк» на основе технологии «толстого клиента»

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

Формой контроля знаний по дисциплине «Защищённые электронные технологии банка» являются две текущие аттестации в виде тестов и итоговая аттестация в виде экзамена.

Неделя текущего контроля	Вид оценочного средства	Код компетенций, оценивающий знания, умения, навыки	Содержание оценочного средства	Требования к выполнению	Срок сдачи (неделя семестра)	Критерии оценки по содержанию и качеству с указанием баллов
Проводится в сроки, установленные графиком	тестирование	ПК-1,2	20 вопросов	Компьютерное тестирование; время отведенное на процедуру - 30 минут	Результаты тестирования предоставляются в день проведения процедуры	

<i>иком образовательно го процесса</i>						
<i>Проводится в сроки, установленные графиком образовательного процесса</i>	тестирование	ПК-1,2	20 вопросов	Компьютерное тестирование; время отведенное на процедуру – 30 минут	Результаты тестирования предоставляются в день проведения процедуры	
<i>Проводится в сроки, установленные графиком образовательного процесса</i>	Экзамен	ПК-1,2	3 вопроса	Экзамен проводится в письменной форме, путем ответа на вопросы. Время, отведенное на процедуру – 30 минут.	Результаты предоставляются в день проведения экзамена	Критерии оценки: « Отлично »: <ul style="list-style-type: none"> • знание основных понятий предмета; • умение использовать и применять полученные знания на практике; • работа на практических занятиях; • знание основных научных теорий, изучаемых предметов; • ответ на вопросы

					билета. «Хорошо»: <ul style="list-style-type: none"> • знание основных понятий предмета; • умение использовать и применять полученные знания на практике; • работа на практических занятиях; • знание основных научных теорий, изучаемых предметов; • ответы на вопросы билета • неправильно решено практическое задание «Удовлетворительно»: <ul style="list-style-type: none"> • демонстрирует частичные знания по темам дисциплин; • незнание неумение использовать и применять полученные знания на практике; • не работал на практических занятиях; «Неудовлетворительно»: <ul style="list-style-type: none"> • демонст
--	--	--	--	--	--

						<p>рирует частичные знания по темам дисциплин;</p> <ul style="list-style-type: none"> • незнание основных понятий предмета; • неумени е использовать и применять полученные знания на практике; • не работал на практически х занятиях; • не отвечает на вопросы.
--	--	--	--	--	--	---

Примерное содержание тестов для текущей аттестации:

ЗАДАНИЕ НА ВЫБОР ОДНОГО ПРАВИЛЬНОГО ВАРИАНТА ОТВЕТА

Тесты используются в режиме промежуточного контроля. По форме заданий выбраны закрытые тесты (с выборочным ответом). Каждому вопросу соответствует один вариант ответа.

1) Из какого материала производят банковские карточки?

- (!) бумажные;
- (!) пластиковые;
- (?) деревянные;
- (!) металлические.

2) В какое время появились карточки с магнитной полосой?

- (?) В 40-е гг XX столетия;
- (?) в 50-е гг XX столетия;
- (!) в 60-е гг XX столетия;
- (?) в 70-е гг XX столетия.

3) Какая операция проводится эмитентом в случае утери карты:

- (?) Держателю карты выносят штраф;

- (!) Номер карты заносится в стоп-лист;
- (?) Эмитент отказывается от сотрудничества с держателем карты.
- (?) Все из вышеперечисленного.

4) Какую операцию выполняет кассир (сотрудник предприятия торговли) при оплате картой в магазине:

- (!) Идентификацию;
- (?) Аутентификацию;
- (!) Авторизацию;
- (?) Все эти операции.

5) Под дебетной картой понимают?

- (!) карта позволяющая рассчитываться в пределах остатка на счете;
- (?) карта позволяющая рассчитываться в пределах установленных лимитов;
- (?) карта позволяющая рассчитываться в пределах как установленных лимитов так и в пределах остатка на счете;
- (?) карта при выдаче которой записывается базовый остаток и дата его возобновления;

6) «Защищенный остаток» памяти микропроцессора предназначен?

- (!) для хранения крупных денежных сумм и проведения расходных операций с предъявлением ПИНа;
- (?) для хранения небольших денежных сумм ;
- (?) для пополнения счета карта без предъявления ПИНа;
- (?) память микропроцессора не содержит «защищенный остаток»;

7) Каким количеством способов может быть проведен этап авторизации при оплате заказных товаров у интернет-магазина?

- (!) 2
- (?) 3
- (?) 5
- (!) 6

8) Хранящиеся на сервере копии электронных документов по всем операциям доступны

- (!) продавцам и покупателям в любой момент времени
- (?) только продавцам в течении 48 часов после проведения операции расчета
- (?) только покупателям в течении 48 часов после проведения операции расчета
- (?) продавцам в любой момент времени

9) Платежная интернет-система ASSIST позволяет

- (!) в реальном времени проводить авторизацию и процессинг платежей, совершаемых при помощи кредитных карт с любого компьютера , подключенного к интернет

(?) в реальном времени проводить авторизацию при помощи кредитных карт с любого компьютера, подключенного к интернет

(?) в реальном времени проводить процессинг платежей, совершаемых при помощи кредитных карт с любого компьютера, подключенного к интернет

(?) верный ответ не представлен

10) Что понимается под системой «Клиент-Банк»:

(!) комплекс, используемый клиентами коммерческого банка и автоматизации документооборота между банком и его клиентами; (?)

(?) комплекс, используемый клиентами некоммерческого банка и автоматизации документооборота

(?) комплекс, не используемый клиентами банка

(?) нет верного варианта

11) Основное назначение системы «Клиент-Банк»:

(!) сократить число визитов клиента в офис банка и формализовать процесс обмена документами

(?) увеличить число визитов клиента в офис банка и формализовать процесс обмена документами

(?) формализовать процесс обмена документами

(?) увеличить количество клиентов

12) Что имеет наибольшее значение для клиента банка в системе:

(!) простота эксплуатации

(!) функциональная полнота системы

(?) простота внедрения

(?) защищенность от НСД

13) Что имеет наибольшее значение для банка при функционировании системы

(?) простота эксплуатации

(?) функциональная полнота системы

(!) простота внедрения

(!) защищенность от НСД

14) Принципиальная особенность системы «Клиент-Банк» на основе технологии «тонкого клиента»:

(!) вся информация передается в банк по мере её ввода клиентом

(?) информация не передаётся в банк по мере ввода клиентом

(?) клиент не вводит информацию в банк

(?) нет верного, вариант

15) Что под собой подразумевает WAP-банкинг:

(!) использование в качестве клиентской части системы мобильного протокола

(?) использование в качестве серверной части системы мобильного протокола

(?) использование в качестве клиентской части системы транспортного протокола

(?) нет правильного варианта

16) Что такое WAP?

(!) протокол, с помощью которого информация из Интернет передаётся на небольшой дисплей мобильного телефона

(?) протокол, с помощью которого информация из Интернет не передаётся на дисплей мобильного телефона

(?) устройство, с помощью которого информация из Интернет передаётся на небольшой дисплей мобильного телефона

(?) протокол, с помощью которого информация передаётся со стационарного телефона на небольшой дисплей мобильного телефона

17) Выбор организации работы клиента с коммерческим банком

зависит от факторов:

(?) удаленность клиента от офиса банка

(?) наличие коммуникационных каналов

(?) удобство эксплуатации клиентской части системы

(!) количество клиентов банка

18) Расшифруйте аббревиатуру WAP:

(!) Wireless Application Protocol

(?) Wireless Application Prototype

(?) Wireless Application Protection

(?) Windows Application Protocol

19) Что в общем случае подразумевается под интернет-банкингом:

(!) оказание банковских услуг через интернет

(?) оказание банковских услуг через терминал

(?) оказание банковских услуг физическим лицам

(?) оказание банковских услуг юридическим лицам

20) В системе «Клиент-Банк» возможно использование

информационных технологий:

(!) тонкий клиент

(!) толстый клиент

(?) умеренный клиент

(?) полный клиент

21) Два основных типа каналов связи:

(!) коммутируемый

(!) выделенный

(?) бронированный

(?) воздушный

22) Типы уровней доступных операций взаимодействия клиента с банком:

(!) информационный

(!) транзакционный

(?) биологический

(?)социальный

23) Что подразумевается под SMS-банкингом:

(!)возможность заказывать и получать информацию посредством SMS-сообщений одного из провайдеров мобильной связи

(?) возможность блокировать информацию посредством SMS-сообщений одного из провайдеров мобильной связи

(?) возможность только заказывать и получать денежные средства посредством SMS-сообщений одного из провайдеров мобильной связи

(?) нет правильного ответа

24) Что подразумевается под переводом в валюты:

(!)ввод формы для осуществления валютного перевода

(?)вывод формы для осуществления валютного перевода

(?)ввод формы для осуществления текстового перевода

(?) ввод формы для осуществления оплаты услуг ЖКХ

25) Что подразумевается под обменными операциями:

(!) операции по конвертации из одной валюты в другую

(?)операции по конвертации из одной валюты в ту же валюту

(?)операции по конвертации валового продукта

(?)нет правильного варианта

26) Что подразумевается под регулярными платежами:

(!) возможность заказа регулярных платежей со своего счёта на другие счета

(?) возможность заказа регулярных платежей с чужого счёта

(?) не возможность заказа регулярных платежей со своего счёта на другие

(?)возможность периодического пополнения своего счета

27) Уровни поддержки решений для интернет - банкинга:

(?) Базовый

(?)Расширенный

(?)Полная

(!)все варианты верны

28) Суть классической системы «Клиент-Банк» с «толстым клиентом»:

(!)на стороне клиента устанавливается специальное программное обеспечение, которое является частью БИС

(?) на стороне банка устанавливается специальное программное обеспечение, которое является частью БИС

(?)на стороне клиента устанавливается антивирусное программное обеспечение

(?)нет правильного варианта

29) Расшифруйте аббревиатуру БИК:

(!)банковский идентификационный код

- (?) банковский интернет-клиент
- (?) банковские, информационный коммуникации
- (?) белорусский интернет-клиент

30) Под расчётами, в рамках какой-либо коммерческой сделки, заключаемой в устной или письменной форме понимается:

- (!) технология проведения оплаты.
- (?) способ передачи денежных средств
- (?) способ взаимодействия клиента с банком
- (?) технология проведения расчётов

31) Межбанковский расчёт отличается от межхозяйственных:

- (!) количественными и качественными характеристиками (?)
- (?) формой проведения
- (?) суммой денег, вовлечённых в расчёт
- (?) участием банка в операции

32) Безналичный расчёт осуществляется через:

- (!) Посредника
- (?) Брокера
- (?) Юриста
- (?) Банк

33) Безналичные расчёты бывают:

- (!) С платёжным поручением
- (!) С платёжным требованием
- (?) С платёжными транзакциями
- (?) С платёжными рисками

34) Телефонный банкинг выделяется за счёт:

- (!) Использования базовых телефонных функций
- (?) Возможностью мобильного использования банка
- (?) Использования базовых компьютерных функций
- (?) Развития информационных технологий

35) Система клиент-банк организует:

- (!) Электронный документооборот между банками и его клиентами
- (?) Электронный документооборот между банками
- (?) Электронный документооборот между клиентами
- (?) Электронный документооборот между контрагентами

36) Система клиент-банк основывается на технологии:

- (!) Тонкий клиент
- (!) Толстый клиент
- (?) Платёжный клиент
- (?) Онлайн клиент

37) Электронный чек отличается от бумажного:

- (!) Формой представления
- (?) Информативностью
- (?) Идентификаторами

- (?)Все вышеперечисленным
- 38) Какие факторы в большей степени влияют на платёжные интернет-системы:**
- (!)Экономические потребности
 - (?)Технологические возможности
 - (?)Правовая база
 - (?)Состоянием экономики
- 39) В традиционных формах расчёта все формы безналичных расчётов выполняются через:**
- (!)Финансового посредника
 - (?)Маклера
 - (?)Брокера
 - (?)Банк
- 40) В основе внешних информационных взаимодействий коммерческого банка лежат:**
- (!)Компьютерные сети
 - (?)Телефонные сети
 - (?)Банковские сети
 - (?)Телекоммуникационные сети
- 41) Международные расчёты выполняются через систему:**
- (!)SWIFT
 - (?)RINET
 - (?)EDIFER
 - (?)OEDIPE
- 42) При разработке «Стандарты публикации финансовой отчётности коммерческих банков» в качестве начального стандарта была выбрана спецификация языка:**
- (!)XBRL
 - (?)XLRB
 - (?)LBRL
 - (?)RBXL

Типовые вопросы, выносимые на экзамен

1. Понятия и концепция информационной безопасности банка.
2. Банк как объект защиты информации.
3. Система информационных угроз безопасности банка.
4. Банк как субъект борьбы с противоправными посягательствами (информационный аспект).
5. Система правового обеспечения информационной безопасности банка.
6. Правовые акты общего действия, обеспечивающие безопасность банков методами охранительного содержания.

7. Банковское законодательство: Нормативные акты Банка России и стандарт ИБ банка России.
8. Содержание аудита по ИБ технических средств обработки информации.
9. Организация системы информационной безопасности банка.
10. Субъекты обеспечения информационной безопасности банка.
11. Средства и методы обеспечения безопасности банка.
12. Организация внутреннего контроля банка (аспект ЗИ).
13. Организация службы информационной безопасности банка.
14. Система технических средств информационной безопасности банка.
15. Технические средства охраны банковских операций и продуктов.
16. Техничко – криминалистические средства защиты информации банка.
17. Защита от хищения денежных средств при совершении кредитных операций.
18. Защита от хищения денежных средств с незаконным использованием пластиковых карт.
19. Защита от хищения денежных средств с использованием аккредитивов.
20. Защита от хищения денежных средств с использованием чеков.
21. Защита от хищения денежных средств с использованием платежных поручений.
22. Правовая характеристика векселя и особенности ее защиты.
23. Риски в сфере вексельного обращения и их информационная безопасность.
24. Преступления против собственности, в которых вексель является предметом посягательств (аспект ЗИ).
25. Меры предупреждения преступлений в сфере вексельного обращения (аспект ЗИ).
26. Злоупотребления полномочиями (аспект ЗИ).
27. Коммерческий подкуп (аспект ЗИ).
28. Противоправные посягательства на сведения банка, составляющие банковскую, коммерческую и служебную тайну (аспект ЗИ).
29. Противоправные посягательства в сфере компьютерного обеспечения деятельности банка (аспект ЗИ).
30. Противоправные посягательства на кадровое обеспечение банка. Противоправные посягательства на нематериальные активы банка (аспект ЗИ).
31. Понятие и правовая характеристика легализации (отмывания) доходов, полученных преступным путем (аспект ЗИ).
32. Криминалистическая характеристика легализации отмывания преступных доходов (аспект ЗИ).
33. Информационная безопасность и система мер предупреждения легализации (отмывания) доходов, полученных преступным путем, и финансирования терроризма.

34. Информация, используемая в целях обеспечения информационной безопасности банка, и ее источники.

35. Бюро кредитных историй (аспект ЗИ).

36. Специальные аналитические технологии для предупреждения и расследования противоправных посягательств на информационную безопасность банка.

**Итоговое начисление баллов по дисциплине осуществляется в соответствии с разработанной и внедренной балльно-рейтинговой системой контроля и оценивания уровня знаний и внеучебной созидательной активности обучающихся.*

**Методические указания для обучающихся по освоению дисциплины
(модуля)**

**ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И
ТЕХНОЛОГИЙ**

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО
ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)**

«ЗАЩИЩЕННЫЕ ЭЛЕКТРОННЫЕ ТЕХНОЛОГИИ БАНКА»

Направление подготовки: 10.03.01 «Информационная безопасность»

Профиль: Организация и технологии защиты информации

Уровень высшего образования: бакалавриат

Форма обучения: очная, очно-заочная

Королев
2023

1. Общие положения

Целями изучения дисциплины является:

- Ускоренная адаптация студентов в предметную область информационная безопасность, опираясь на весь спектр научных воззрений, на развитие и защиту информационно - телекоммуникационной инфраструктуры и компьютерной информации в кредитно – финансовой сфере;
- Повысить уровень специальных знаний, которые необходимы обучающимся для высоко профессиональной деятельности во всех сферах информационной безопасности с учетом требований высшей школы, для активизации их учебной и исследовательской деятельности;
- Формирование у студентов специализированной базы знаний по основным понятиям в области информационной безопасности банковской деятельности;
- Приобретение студентами первичных навыков по практическому формированию комплекса документов, составляющих правовую базу защиты информации в банковской сфере.

Задачами дисциплины являются:

1. ознакомить студентов с задачами в области безопасности банковской деятельности на основе действующего российского законодательства;
2. научить студентов самостоятельно решать поставленные задачи в области защиты информации в банках по базовым направлениям защиты банковской тайны и конфиденциальной информации;
3. формировать систему знаний у обучающихся в области защиты информации в кредитно финансовой сфере деятельности.
4. изучить основы организации противодействия угрозам информационной безопасности в кредитно – финансовой сфере;
5. ознакомить с системным описанием внешних угроз безопасности кредитно – финансовой деятельности, правовых и организационных основ противодействия им, а также техники обеспечения безопасности кредитно – финансовой организации;
6. ознакомить с методами и средствами защиты информации банковских инструментов и технологий функциональных и контролирующих подразделений финансово – кредитных организаций.

2. Указания по проведению практических занятий

Тема 1. Концептуальные основы информационной безопасности банка

Практическое занятие 1.

Вид практического занятия: *подготовка доклада.*

Образовательные технологии: *групповая дискуссия.*

Вид практического занятия: *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки моделирования основных угроз безопасности банка.

Основные положения темы занятия:

1. базовые составляющие концепции информационной безопасности банка.
2. основные направления обеспечения информационной безопасности банковской деятельности.

Вопросы для обсуждения:

- а) Основной доклад (реферат) по теме занятия.
 1. Понятия и концепция информационной безопасности банка.
 2. Банк как объект противоправных посягательств.
 3. Система информационных угроз безопасности банка.
 4. Банк как субъект борьбы с противоправными посягательствами.

Продолжительность занятия – 1/1 ч.

Тема 2. Правовые основы информационной безопасности банка

Практическое занятие 2.

Вид практического занятия: *подготовка доклада.*

Образовательные технологии: *групповая дискуссия.*

Вид практического занятия: *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки моделирования основных угроз безопасности банка в соответствии с требованиями законодательства.

Основные положения темы занятия:

1. базовые составляющие правового обеспечения информационной безопасности банка.
2. стратегия информационной безопасности типового банка.

Вопросы для обсуждения:

- а) Основной доклад (реферат) по теме занятия.
 1. Система правового обеспечения безопасности банка.

2. Правовые акты общего действия, обеспечивающие безопасность банков методами охранительного содержания.
 3. Банковское законодательство.
 4. Нормативные акты Банка России.
 5. Внутренние нормативные акты.
 6. Содержание аудита по информационной безопасности технических средств обработки информации.
- Продолжительность занятия – 1/1 ч.

Тема 3. Организационные основы информационной безопасности банка

Практическое занятие 3.

Вид практического занятия: **подготовка доклада.**

Образовательные технологии: **групповая дискуссия.**

Вид практического занятия: *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки организации работы типовых структурных подразделений службы безопасности банка.

Основные положения темы занятия:

1. базовые составляющие организационного обеспечения информационной безопасности банка.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

1. Организация системы безопасности банка.

2. Субъекты обеспечения безопасности банка.

3. Средства и методы обеспечения безопасности банка.

Организация внутреннего контроля банка.

4. Организация службы безопасности банка.

Продолжительность занятия – 1/1 ч.

Тема 4. Техника обеспечения информационной безопасности банка

Практическое занятие 4.

Вид практического занятия: **подготовка доклада.**

Образовательные технологии: **групповая дискуссия.**

Вид практического занятия: *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки организации работы типовых структурных подразделений службы безопасности банка.

Основные положения темы занятия:

1. технические средства охраны банка.

2. безопасность банковских расчетов

Вопросы для обсуждения:

- а) Основной доклад (реферат) по теме занятия.
1. Система технических средств информационной безопасности банка. Технические средства охраны.
 2. Технические средства охраны банковских операций и продуктов.
 3. Техничко – криминалистические средства.
- Продолжительность занятия – 1/1 ч.

Тема 5. Защита от информационных преступлений, посягающих на собственность банка

Практическое занятие 5.

Вид практического занятия: **подготовка доклада.**

Образовательные технологии: **групповая дискуссия.**

Вид практического занятия: *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки организации работы службы безопасности по проведению расследований инцидентов информационной безопасности.

Основные положения темы занятия:

1. Характеристика преступлений связанных с хищением денежных средств.
2. безопасность банковских расчетов

Вопросы для обсуждения:

- а) Основной доклад (реферат) по теме занятия.
1. Хищения денежных средств при совершении кредитных операций.
 2. Хищения денежных средств с незаконным использованием пластиковых карт.
 3. Хищения денежных средств с использованием аккредитивов.
 4. Хищение денежных средств с использованием чеков. Хищение денежных средств с использованием платежных поручений.
- Продолжительность занятия – 1/1 ч.

Тема 6. Стандарты информационной безопасности банка

Практическое занятие 6.

Вид практического занятия: **подготовка доклада.**

Образовательные технологии: **групповая дискуссия.**

Вид практического занятия: *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки организации учета требований стандартов информационной безопасности банка.

Основные положения темы занятия:

1. Характеристика российских и международных стандартов банковской деятельности.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

1. О Стандарте Банка России “Обеспечение информационной безопасности организаций банковской системы Российской Федерации.

Общие положения.

2. Основные цели и задачи стандарта Банка России при обеспечении информационной безопасности.

3. Основные направления работы по дальнейшему сопровождению и доработке Стандарта в рамках специально созданного Подкомитетом 3 “Защита информации в кредитно-финансовой сфере” Технического комитета 362 “Защита информации” Федерального агентства по техническому регулированию и метрологии.

4. Аудит информационной безопасности банка.

5. Преимущества и недостатки выполнения работ по защите ПДн в рамках Стандарт Банка России СТО БР ИББС 1.0-2014.

Продолжительность занятия – 1/1 ч.

Тема 7. Хищения денежных средств и иного имущества с использованием векселей (информационный аспект)

Практическое занятие 7.

Вид практического занятия: **подготовка доклада.**

Образовательные технологии: **групповая дискуссия.**

Вид практического занятия: **смешанная форма практического занятия.**

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки в противодействии хищения денежных средств в сфере вексельного обращения.

Основные положения темы занятия:

1. Противодействие хищению денежных средств и иного имущества с использованием векселей.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

1. Правовая характеристика векселя. Риски в сфере вексельного обращения.

2. Преступления против собственности, в которых вексель является предметом посягательств.

3. Преступления против собственности, в которых вексель является средством совершения преступления.

4. Меры предупреждения преступлений в сфере вексельного обращения.

Продолжительность занятия – 1/1 ч.

Тема 8. Защита от информационных преступлений, посягающих на информационную безопасность функционирования банка
Практическое занятие 8.

Вид практического занятия: **подготовка доклада.**

Образовательные технологии: **групповая дискуссия.**

Вид практического занятия: *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки в защите от информационных преступлений.

Основные положения темы занятия:

1. Противодействие преступлениям, посягающим на информационную безопасность банка.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

1. Злоупотребления полномочиями.

2. Коммерческий подкуп.

3. Противоправные посягательства на сведения банка, составляющие банковскую, коммерческую и служебную тайну.

4. Противоправные посягательства в сфере компьютерного обеспечения деятельности банка.

5. Противоправные посягательства на кадровое обеспечение банка.

6. Противоправные посягательства на нематериальные активы банка.

Продолжительность занятия – 1/1 ч.

Тема 9. Организация противодействия отмыванию преступных доходов и финансированию терроризма (информационный аспект)
Практическое занятие 9.

Вид практического занятия: **подготовка доклада.**

Образовательные технологии: **групповая дискуссия.**

Вид практического занятия: *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки в противодействии отмыванию доходов полученных преступным путем.

Основные положения темы занятия:

1. Противодействие преступлениям, связанным с отмыванием доходов полученных преступным путем и финансированием терроризма.

Вопросы для обсуждения:

- а) Основной доклад (реферат) по теме занятия.
1. Понятие и правовая характеристика легализации (отмывания) доходов, полученных преступным путем.
 2. Криминалистическая характеристика легализации (отмывания) преступных доходов).
 3. Система мер предупреждения легализации (отмывания) доходов, полученных преступным путем, и финансирования терроризма.
- Продолжительность занятия – 1/1 ч.

Тема 10. Комплексное обеспечение информационной безопасности банка

Практическое занятие 10.

Вид практического занятия: *подготовка доклада.*

Образовательные технологии: *групповая дискуссия.*

Вид практического занятия: *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки в формировании комплексной системы информационной безопасности банка.

Основные положения темы занятия:

1. Основные требования предъявляемые к системе обеспечения банковской деятельности.

Вопросы для обсуждения:

- а) Основной доклад (реферат) по теме занятия.
1. Информация, используемая в целях обеспечения безопасности банка, и ее источники.
 2. Бюро кредитных историй.
 3. Специальные аналитические технологии для предупреждения и расследования противоправных посягательств на безопасность банка.

Продолжительность занятия – 7/2 ч.

4. Указания по проведению самостоятельной работы студентов

№ п/п	Наименование блока (раздела) дисциплины	Виды СРС
1.	Тема 7. Защита от хищения денежных средств и иного имущества с использованием векселей (информационный	<i>Подготовка докладов по темам:</i> 1. Информационная безопасность подсистемы ведения индивидуальных счетов клиентов. 2. Информационная безопасность подсистемы работы с банковскими картами. 3. Информационная безопасность подсистемы

	аспект)	кредитования и подсистема валютно – обменных операций. 4. Информационная безопасность подсистема операций с ценными бумагами.
2.	Тема 8. Защита от информационных преступлений, посягающих на информационную безопасность функционирования банка	Подготовка докладов по темам: 1. Информационная безопасность подсистема инкассации и подсистемы межбанковского взаимодействия. 2. Информационная безопасность подсистемы управления ресурсами (диллинга). 3. Информационная безопасность в подсистеме обеспечения безопасности. 4. Информационная безопасность подсистемы генерации отчетов, планирования и анализа деятельности.
3	Тема 9. Организация противодействия отмыванию преступных доходов и финансированию терроризма (информационный аспект)	Подготовка докладов по темам: 1. Информационная безопасность подсистема удаленного банковского обслуживания. 2. Информационная безопасность подсистема обеспечения внутренней деятельности банка как субъекта экономики. 3. Информационная безопасность системы электронного документооборота банка. 4. Информационная безопасность традиционных технологий расчетов. 5. Информационная безопасность и архитектура системы «Клиент – банк».
4	Тема 10. Комплексное обеспечение информационной безопасности банка	Подготовка докладов по темам: 1. Информационная безопасность и способы передачи информации до компьютерной сети банка. 2. Информационная безопасность системы телефонного банкинга. 3. Информационная безопасность системы «Клиент – банк» на основе технологии «толстого клиента» 4. Информационная безопасность модели Интернет - банкинга.

5. Указания по проведению контрольных работ

5.1. Требования к структуре

Структура контрольной работы должна способствовать раскрытию темы: иметь титульный лист, содержание, введение, основную часть, заключение, список литературы.

5.2. Требования к содержанию (основной части)

1. Во введении обосновывается актуальность темы, определяется цель работы, задачи и методы исследования.

2. При определении целей и задач исследования необходимо правильно их формулировать. Так, в качестве цели не следует употреблять глагол «сделать». Правильно будет использовать глаголы «раскрыть», «определить», «установить», «показать», «выявить» и т.д.

3. Основная часть работы включает 2-4 вопроса, каждый из которых посвящается решению задач, сформированных во введении, и заканчивается констатацией итогов.

4. Приветствуется иллюстрация содержания работы таблицами, графическим материалом (рисунками, схемами и т.п.).

5. Необходимо давать ссылки на используемую литературу.

6. Заключение должно содержать сделанные автором работы выводы, итоги исследования.

7. Вслед за заключением идет список литературы, который должен быть составлен и оформлен с установленными требованиями. Если в работе имеются приложения, они оформляются на отдельных листах, и должны быть соответственно пронумерованы.

5.3. Требования к оформлению

Объём контрольной работы – 5-6 страниц формата А4, напечатанного с одной стороны текста (1,5 интервал, шрифт Times New Roman).

5.4. Примерная тематика контрольных работ:

1. Информационная безопасность системы «Клиент – банк» на основе технологии «толстого клиента»
2. Информационная безопасность модели Интернет - банкинга.
3. Информационная безопасность расчетов банковскими картами в Интернете.
4. Место ЭЦП в ряду криптографических механизмов. История возникновения ЭЦП в России. Общее правило создания ЭЦП. Общее правило верификации ЭЦП.
5. Схема защищенного информационного обмена при использовании симметричных методов защиты информации.

6. Схема защищенного информационного обмена при использовании криптографических алгоритмов с открытыми ключами.
7. Применение и информационная безопасность режима электронной кодовой книги. Режим сцепления блоков шифротекста. Режим обратной связи по шифротексту.
8. Режим счетчика (counter). Функция хеширования и асимметричные алгоритмы.
9. Информационная безопасность и защита электронных транзакций протокол (SSL). Схема работы протокола SET.
10. Информационная безопасность электронных платежей с помощью цифровых денег.
11. Информационная безопасность расчетной функции банков и ее автоматизации. Схема обработки платежного документа клиентами.
12. Информационная безопасность и ключевые принципы для системно – значимых платежных систем. Определение количества ресурсов, которые банк будет держать на своих корсчетах.
13. Информационная безопасность и правила обмена электронными документами. Общие требования, предъявляемые к ЭД (пакетам ЭД).
14. Информационная безопасность при составление и направление ЭД участником – отправителем.
15. Информационная безопасность и порядок контроля ЭД, полученных от участников – отправителей. Порядок оформления ЭД, подтверждающих исполнение ЭД участников.
16. Информационная безопасность и порядок приема к исполнению ЭД участником – получателем. Порядок хранения и уничтожения ЭД.

6. Перечень основной и дополнительной учебной литературы

Основная литература:

1. Кибербезопасность в условиях электронного банкинга : практическое пособие / под ред. П. В. Ревенкова. - Москва : Прометей, 2020. - 522 с. - ISBN 978-5-907244-61-0. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1284190> (дата обращения: 28.11.2022). – Режим доступа: по подписке.
2. Бабаш, А. В. Моделирование системы защиты информации. Практикум : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 3-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 320 с. + Доп. материалы [Электронный ресурс]. — (Высшее образование). — DOI: <https://doi.org/10.29039/01848-4>. - ISBN 978-5-369-01848-4. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1232287> (дата обращения: 28.11.2022). – Режим доступа: по подписке.

Дополнительная литература:

3. Тавасиев, А. М. Банковское кредитование : учебник / А.М. Тавасиев, Т.Ю. Мазурина, В.П. Бычков ; под ред. А.М. Тавасиева. — 2-е изд., перераб. —

Москва : ИНФРА-М, 2020. — 366 с. — (Среднее профессиональное образование). - ISBN 978-5-16-014239-5. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1039295> (дата обращения: 28.11.2022). – Режим доступа: по подписке.

7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

Интернет-ресурсы:

1. <http://eup.ru/catalog/all-all.asp> – научно-образовательный портал.
2. <http://informika.ru/> – образовательный портал.
3. www.wikIsec.ru - Энциклопедия информационной безопасности. –

Публикации, статьи.

4. www.biblioclub.ru - Универсальная библиотека онлайн.
5. www.rucont.ru - ЭБС «Руконт».
6. <http://www.academy.it.ru/> – академия АЙТИ.
7. <http://www.minfin.ru> - Официальный сайт Министерства финансов Российской Федерации
8. <http://www.gov.ru> - Официальный сервер органов государственной власти Российской Федерации.
9. <http://www.fsb.ru/> - Официальный сайт Федеральной Службы Безопасности
- 10 <http://www.fstec.ru/> - Официальный сайт Федеральной Службы по Техническому Экспортному контролю

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю)

Перечень программного обеспечения: MSOffice, PowerPoint.

Информационные справочные системы:

1. Электронные ресурсы образовательной среды Университета.
2. Информационно-справочные системы (Консультант+; Гарант).
3. Рабочая программа и методическое обеспечение по курсу: «Защищенные электронные технологии банка»