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

Троицкий Александр Витальевич

Подписано цифровой подписью: Троицкий Александр Витальевич

«УТВЕРЖДАЮ»
И.о. проректора
_____ А.В. Троицкий
«___»_____2023 г.

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.В.ДВ.03.01 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ФИНАНСОВО-КРЕДИТНЫХ СТРУКТУР»

Направление подготовки: 10.04.01 - Информационная безопасность
Направленность (профиль): Менеджмент информационной безопасности
Уровень высшего образования: Магистратура
Форма обучения: очная

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 (модуля): Информационная безопасность финансово-кредитных структур. – 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 магистров 10.04.01 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)	Соляной В.Н., к.в.н. доцент			
Год утверждения (переутверждения)	2023	2024		
Номер и дата протокола заседания кафедры	№8 от 29.03.2023г.			

Рабочая программа согласована:
Руководитель ОПОП ВО Сухотерин А.И.

Рабочая программа рекомендована на заседании УМС:

Год утверждения (переутверждения)	2023	2024		
Номер и дата протокола заседания УМС	№5 от 11.04.2023г.			

2

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения ОПОП

Целью изучения дисциплины являются:

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 необходимых 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 по направлению подготовки 10.04.01 «Информационная безопасность», студент приобретает и совершенствует следующие компетенции:

Профессиональные компетенции:

- ПК-1: Способен организовывать выполнение работ, управлять коллективом автоматизированных ИАС в защищенном исполнении.
- ПК-2: Способен разрабатывать проектные решения по развитию автоматизированных ИАС в защищенном исполнении.

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:

Трудовые действия:

- ПК-1.3. Управлять работой коллектива профессионалов ИБ, разрабатывать нормативно-методические документы по функционированию автоматизированной ИАС, формировать комплекс мер по информационной защите автоматизированной ИАС с разработкой частных политик безопасности компьютерных систем.
- ПК-2.3. Разрабатывать проекты документов по созданию защищенных технологий с оформлением технических заданий на проектирование, осуществлять непосредственную разработку проектных решений по ИБ и оценку их эффективности в автоматизированной ИАС.

Необходимые умения:

- ПК-1.2. Работать в коллективе, разрабатывать организационно-управленческие документы, принимать управленческие решения, реализовывать целесообразные меры противодействия информационным угрозам с применением национальных и международных стандартов в области ЗИ, оценивать их эффективность.
- ПК-2.2. Проводить предпроектное обследование с выбором перспективной технологии защиты автоматизированной ИАД с разработкой проектной документации и комплексной оценкой эффективности применения автоматизированной ИАС.

Необходимые знания:

- ПК-1.1. Знать научные основы, методы и технологии управленческой деятельности, нормативную базу по созданию и эксплуатацию защищенных автоматизированных ИАС, принципы и методы организации работ по ЗИ в ИАС, основные средства и способы организационного обеспечения ИБ, источники и классификацию угроз ИБ.
- ПК-2.1. Знать нормативную базу создания и эксплуатации защищенных функциональных и обеспечивающих подсистем, методы проектирования, критерии и показатели эффективности, автоматизированной ИАС.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОПОП ВО

Дисциплина «Информационная безопасность финансово-кредитных структур» Б1.В.ДВ.03.01 относится к дисциплинам по выбору части, формируемой участниками образовательных отношений, блока 1 основной профессиональной образовательной программы подготовки магистров по направлению подготовки 10.04.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Дисциплина базируется на ранее изученных дисциплинах: ”Экономика и управление”, “Основы теории информационной безопасности“, “Защищённые информационные системы“ и компетенциях: УК-1, 2; ПК-1, 3; ОПК-1.

Знания и компетенции, полученные при освоении дисциплины «Теоретические основы компьютерной безопасности» являются базовыми для изучения последующих дисциплин «Информационно-аналитические системы безопасности», «Информационная безопасность финансово-кредитных структур», «Компьютерное моделирование информационных процессов и технологий» прохождения практики (НИР), государственной итоговой аттестации и выполнения выпускной квалификационной работы (магистерской диссертации).

3. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины для студентов очной формы составляет 2 зачетных единицы, 72 часа.

Таблица1

Виды занятий	Всего часов	Семестр 3	Семестр 8	Семестр …	Семестр …
Общая трудоемкость	72	72			
ОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	46	46			
Лекции (Л)	16	16			
Практические занятия (ПЗ)	16	16			
Лабораторные работы (ЛР)	**8**	**8**			
Практическая подготовка	**4**	**4**			
Другие виды контактной работы*	6	6			
Самостоятельная работа	26	26			
Курсовые работы (проекты)	-	-			
Расчетно-графические работы	-	-			
Контрольная работа, домашнее задание	+ -	+ -			
Текущий контроль знаний (7 - 8, 15 - 16 недели) – 2ч	нет	нет			
Вид итогового контроля	Зачет	Зачет			

* 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.	Практ. занят., час.	Лабораторные заняти я час.	Занят. в интеракт. форме, час.	Практическая поготовка ,час	Код компетенций
Раздел 1. Организационные основы ИБ региональных финансово –кредитных структур						
Введение. Концептуальные основы информационной безопасности региональных финансово-кредитных организаций	2	1	нет	1		ПК-1
Тема 2. Организационные и правовые основы информационной безопасности	2	1	нет	1		ПК-1
Тема 3. Стандарты информационной безопасности финансово – кредитных организаций	2	1	1	1		ПК-1
Тема 4. Техника обеспечения информационной безопасности финансово – кредитных организаций	2	1	1	1		ПК-1,2
Тема 5. Защита от информационных преступлений, посягающих на собственность финансово – кредитных организаций	2	1	1	1		ПК-1
Тема 6. Информационная безопасность электронных транзакций и электронных расчетов в финансово –	2	2	1	1		ПК-1

кредитной деятельности						
Раздел II. Технологии защиты информации в финансово – кредитной деятельности						
Тема 7. Защита от хищения денежных средств и иного имущества с использованием векселей (информационный аспект)	2	2	1	1	1	ПК-1,2
Тема 8. Защита от информационных преступлений, посягающих на информационную безопасность функционирования финансово – кредитных структур	1	2	1	1	1	ПК-1,2
Тема 9. Организация противодействия отмыванию преступных доходов и финансированию терроризма (информационный аспект)	0.5	2	1	1	1	ПК-1,2
Тема 10. Способы оценки информации. Обеспечение безопасности и защиты информации. Специальные аналитические технологии для предупреждения и расследования противоправных посягательств на безопасность в органах государственной власти и местного самоуправления	0.5	3	1	2	1	ПК-1,2
Итого:	**16**	**16**	**8**	**12**	**4**	

4.2. Содержание тем дисциплины

Тема 1. Введение. Концептуальные основы информационной безопасности региональных финансово-кредитных организаций

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

Тема 2. Организационные и правовые основы информационной безопасности финансово кредитных структур

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.

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

Тема 3. Стандарты информационной безопасности финансово – кредитных организаций

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.

Тема 4. Техника обеспечения информационной безопасности финансово – кредитных организаций

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

Тема 5. Защита от информационных преступлений, посягающих на собственность финансово – кредитных организаций

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.

Тема 6. Информационная безопасность электронных транзакций и электронных расчетов в финансово – кредитной деятельности

Традиционные технологии расчетов и их автоматизированные (электронные) формы. Классификация расчетов по субъектам и формам. Структурная схема взаимодействия традиционных и автоматизированных (электронных) форм расчетов. Информационные технологии внешних взаимодействий КБ.

Основные понятия. Схема защищенного информационного обмена при использовании симметричных методов. Схема защищенного информационного обмена при использовании криптографических алгоритмов с открытыми ключами. Симметричные алгоритмы шифрования. Схема алгоритма работы сети Фейсталя. Режим электронной кодовой книги. Режим сцепления блоков шифротекста. Режим обратной связи по шифротексту. Режим обратной связи по выходу. Режим счетчика (counter). Функция хеширования и асиметричные алгоритмы.

Раздел II. Технологии защиты информации в финансово – кредитной 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 финансово – кредитных структур

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.

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. Способы оценки информации. Обеспечение безопасности и защиты информации. Специальные аналитические технологии для предупреждения и расследования противоправных посягательств на безопасность в органах государственной власти и местного самоуправления

Источники информации. Обретение доступа к документам. Перехват и перлюстрация писем. Обработка «мусора». Техника интерпретации данных. Обеспечение безопасности и защиты информации. Специальные аналитические технологии для предупреждения и расследования противоправных посягательств на безопасность

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

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

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

Структура фонда оценочных средств, для проведения промежуточной аттестации обучающихся по дисциплине «Информационная безопасность кредитно-финансовых структур» приведена в Приложении 1.

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

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 (модуля)

Интернет-ресурсы:

1. **http://eup.ru/catalog/all-all.asp – научно-образовательный портал.**
2. **http://informika.ru/ – образовательный портал.**
3. **http://www.academy.it.ru/ – академия АЙТИ.**

9. Методические указания для обучающихся, по освоению дисциплины (модуля)

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

10. 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)

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.

Самостоятельная работа студентов может проводится, как в специально оборудованных компьютерных классах университета с выходом в Интернет, так и в домашних условиях при наличии Интернет – сети.

Задание.

ЗАДАЧА 1.

Холдинговая компания «ПОЛИМЕТ» имеет головное предприятие и несколько дочерних фирм в ряде городов России и за рубежом. В структуру холдинга входит коммерческий банк. Основной деятельностью «ПОЛИМЕТА» является переработка металлургического сырья, производство изделий из металла, торговля сырьем и изделиями из металла. Головным предприятием владеют несколько человек. Они же владеют контрольными пакетами акций всех дочерних предприятий. Обороты холдинга исчисляются миллиардами рублей. На рынке металла, как в стране, так и за рубежом идет жесткая конкуренция. Условия торговли металлами предельно строгие и требуют постоянного взаимодействия с контролирующими и проверяющими органами. Необходимо постоянное оформление квот, лицензий и других разрешительных документов. Торговля металлами требует больших объемов железнодорожных и морских перевозок.

ВОПРОСЫ:

- 1. Какие задачи могут стоять перед Службой Конкурентной Разведки (СКР) исходя из условий работы холдинга, его структуры, оборотов, особенностей рынка?
- 2. Какая оптимальная структура Службы Конкурентной Разведки может быть выбрана в соответствии с определенными для СКР задачами?

ЗАДАЧА 2.

Фирма «ЛИНДА» занимается оказанием информационных и консалтинговых услуг в области новых технологий. Основное внимание уделяет конверсионным разработкам, нс имеющим аналогов в мире. Она собирает информацию о наиболее перспективных научных разработках, позволяющих наладить производство высоко ликвидной на западном рынке продукции.

Фирма занимается привлечением инвестиций, решает вопросы оформления патентов на изобретения и организации производства.

В фирме работает небольшой штат (20 человек) постоянных сотрудников и привлекается более 100 специалистов по трудовым соглашениям.

ВОПРОСЫ:

- 1. Какие задачи могут стоять перед Службой Конкурентной Разведки исходя из условий работы фирмы, ее структуры, особенностей рынка?
- 2. Какая оптимальная структура СКР может быть выбрана в соответствии с определенными для СКР задачами?

ЗАДАЧА 3.

Производственно-коммерческая фирма «АВЕКС» решила создать СКР для защиты своих интересов. Вас пригласили создать СКР и организовать ее работу для решения следующих задач:

физической охраны помещений и защиты руководителей от конкурентной разведки;

инженерной защиты офиса и производственных помещений от несанкционированного доступа конкурентов к информационным ресурсам фирмы;

информационного освещения деятельности партнеров и конкурентов, в том числе зарубежных.

ВОПРОС:

Какие предприятия и организации вы хотели бы привлечь к работе, и какие вопросы вы предполагаете решать с ними?

ЗАДАЧА 4.

Холдинговая компания «Глобус» специализируется на международных транспортных перевозках. В одном из западноевропейских дочерних предприятий, работающих в тесном партнерстве с предприятием, расположенном в российском порту, произошло чрезвычайное происшествие - покушение на директора. Директор тяжело ранен. Состояние дел в предприятии неважное: прибыли нет, большая текучесть кадров.

Руководство холдинга поручило СКР разобраться с положением, защитить интересы фирмы, обеспечить безопасность персонала.

ВОПРОС:

При отработке версий и выполнении задания к кому необходимо было бы обратиться за помощью и какие вопросы решать?

ЗАДАЧА 5.

Торговая компания г. Томска закупила в Москве партию изделий бытовой электроники общим объемом около 5 грузовых автомобилей. По условиям контракта товар продавался со склада в Москве, далее самовывозом. Полную партию товара продавец обязался поставить в течение недели частями.

Покупатель решил везти груз на автомобилях, арендованных в Московских транспортных агентствах.

Охрану груза было поручено осуществлять СБ компании.

ВОПРОС:

Какие меры следует предпринять СБ компании для обеспечения сохранности груза?

ЗАДАЧА 6.

Коммерческий банк «Развитие» по личной рекомендации Председателя союза банков принял в качестве клиента ТОО «Веста», где учредителями были российская гражданка и турецкий гражданин. Через некоторое время турок объявил, что готовит очень крупный контракт по строительству индивидуальных коттеджей и попросил кредит на 40 млн. рублей. Так как в залог он представить ничего не мог, за него выступил с ходатайством «по дружбе» Председатель союза. Еще через некоторое время он попросил кредит на 80 млн. руб. и в качестве залога предложил арендный договор на землю. Получив кредиты, турок перестал вести расчеты через этот банк и вскоре объявил о закрытии фирмы.

Предварительным расследованием СКР банка установлено, что кредит турок использовал на другие нужды. Денег на счету новой фирмы почти нет. Арендный договор на землю был оформлен с грубейшими нарушениями

закона в сговоре с председателем колхоза. В финансовых документах отмечается умышленное искажение отчетности, налоги нс платились. Существенную поддержку турку оказывал бывший руководящий сотрудник правоохранительного министерства.

ВОПРОСЫ:

- 1. Какие предупредительные меры нужно было предпринять СКР в отношении гражданина Турции?
- 2. По каким направлениям следует вести разработку турка, чтобы поставить его перед необходимостью вернуть взятый кредит?

ЗАДАЧА 7.

Агропромышленная фирма «Юниор» имеет головное предприятие в Москве и несколько дочерних фирм в различных регионах России. К руководству фирмы «Юниор» на одной специализированной выставке обратился господин N, представившийся сотрудником известной зарубежной компании «АВС», с предложением об участии в совместном проекте в регионе, в котором «Юниор» имеет дочернюю фирму.

ВОПРОСЫ:

- 1. Какие мероприятия по проверке потенциального зарубежного партнера компании «АВС» должна провести Служба Конкурентной Разведки фирмы «Юниор»?
- 2. На какие моменты необходимо обратить особое внимание?

Приложение 1

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 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ФИНАНСОВО-КРЕДИТНЫХ СТРУКТУР

Направление подготовки: 10.04.01 - Информационная безопасность

Профиль: Менеджмент информационной безопасности

Уровень высшего образования: магистратура

Форма обучения: очная

Королев
2023

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

№ п/п	Индекс компе-тенции	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-2	Способен разрабатывать проектные решения по развитию автоматизированных ИАС в защищенном исполнении.	Тема:1,2,3,5, 6,7,9,10	ПК-2.3. Разрабатывать проекты документов по созданию защищенных технологий с оформлением технических заданий на проектирование, осуществлять непосредственную разработку проектных решений по ИБ и оценку их эффективности в автоматизированной ИАС.	ПК-2.2. Проводить предпроектное обследование с выбором перспективной технологии защиты автоматизированной ИАД с разработкой проектной документации и комплексной оценкой эффективности и применения автоматизированной ИАС.	ПК-2.1. Знать нормативную базу создания и эксплуатации защищенных функциональных и обеспечивающих подсистем, методы проектирования, критерии и показатели эффективности автоматизированной ИАС.
2.	ПК-1	Способен организовывать выполнение работ, управлять коллективом автоматизированных ИАС в защищенном исполнении.	Тема:1,2,3,4, 6,7,8,9	ПК-1.3. Управлять работой коллектива профессионалов ИБ, разрабатывать нормативно-методические документы по функционированию автоматизированной ИАС, формировать комплекс мер по информацион	ПК-1.2. Работать в коллективе, разрабатывать организационно-управленческие документы, принимать управленческие решения, реализовывать целесообразные меры противодействия	ПК-1.1. Знать научные основы, методы и технологии управленческой деятельности, нормативную базу по созданию и эксплуатацию защищенных автоматизированных ИАС, принципы и методы организации

				ной защите автоматизированной ИАС с разработкой частных политик безопасности компьютерных систем	информационным угрозам с применением национальных и международных стандартов в области ЗИ, оценивать их эффективность.	работ по ЗИ в ИАС, основные средства и способы организационного обеспечения ИБ, источники и классификацию угроз ИБ.

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

Код компетенции	*Инструменты, оценивающие сформированность компетенции*	*Этапы и показатель оценивания компетенции*	*Критерии оценивания компетенции на различных этапах формирования и шкалы оценивания*
ПК-1,2	*Тест*	***А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 90% правильных ответов*** ***Б) частично сформирована:*** • ***компетенция освоена на <u>продвинутом</u> уровне – 70% правильных ответов;*** • ***компетенция освоена на <u>базовом</u> уровне – от 51% правильных ответов;*** ***В) не сформирована (<u>компетенция не сформирована</u>) – менее 50% правильных ответов***	***Например:*** ***Проводится письменно. Время, отведенное на процедуру - 30 минут.*** ***Неявка – 0 баллов.*** ***Критерии оценки определяются процентным соотношением.*** ***Неудовлетворительно – менее 50% правильных ответов.*** ***Удовлетворительно - от 51% правильных ответов.*** ***Хорошо - от 70%.*** ***Отлично – от 90%.*** ***Максимальная оценка – 5 баллов.***
ПК-1,2	Доклад	***А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 5 баллов*** ***Б) частично сформирована:*** • ***компетенция освоена на <u>продвинутом</u> уровне – 4 балла;*** • ***компетенция освоена на <u>базовом</u> уровне – 3 балла;*** ***В) не сформирована (<u>компетенция не сформирована</u>) – 2 и менее баллов***	Проводится устно с использованием мультимедийных систем, а также с использованием технических средств Время, отведенное на процедуру – 10 - 15 мин. Неявка – 0. Критерии оценки: 1.Соответствие представленной презентации заявленной тематике (1 балл). 2.Качество источников и их количество при подготовке доклада и разработке презентации (1 балл). 3.Владение информацией и способность отвечать на вопросы аудитории (1 балл). 4.Качество самой представленной презентации (1 балл). 5.Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл). Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся непосредственно в день проведения презентации – для текущего контроля. Оценка проставляется в электронный журнал.
ПК-1,2	Контрольная работа	***А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 90% правильных***	1. Проводится устно в форме защиты отчета 2.Время, отведенное на процедуру – 10 - 15 мин.

		ответов ***Б) частично сформирована:*** • ***компетенция освоена на <u>продвинутом</u> уровне – 70% правильных ответов;*** • ***компетенция освоена на <u>базовом</u> уровне – от 51% правильных ответов;*** ***В) не сформирована (<u>компетенция не сформирована</u>) – менее 50% правильных ответов***	Неявка – 0. Критерии оценки: 1.Соответствие оформления требованиям (1 балл). 2. Соответствие разработанного устройства техническому заданию (1 балл) 3. Моделирование работы разработанного устройства (1 балл) 4. Качество и количество используемых источников (1 балл) 5. Правильность и полнота ответов на контрольные вопросы (1 балл) Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся непосредственно после защиты – для текущего контроля. Оценка проставляется в электронный журнал.
ПК-1,2	Лабораторная работа	А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 5 баллов Б) частично сформирована: • компетенция освоена на <u>продвинутом</u> уровне – 4 балла; • компетенция освоена на <u>базовом</u> уровне – 3 балла; В) не сформирована (<u>компетенция не сформирована</u>) – 2 и менее баллов	Например: 1. Оформление в соответствии с требованиями (1 балл). 2. Выбор методов измерений и вычислений (1 балл). 3. Умение применять выбранные методы (1 балл). 4. Анализ и выводы, отражающие суть изучаемого явления с указанием конкретных результатов (2 балла). Максимальная оценка – 5 баллов.

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 форме презентаций:

1. Нормативно-методологические основы комплексного аудита информационной безопасности.
2. Базовые положения по комплексному аудиту информационной безопасности предприятий (учреждений, организаций) региона.
3. Привлекаемые силы к проведению комплексного аудита ИБ объектов региона.
4. Принципы организации и методы проведения комплексного аудита ИБ.
5. Содержание комплексного аудита ИБ для выделенных помещений.
6. Основные этапы комплексного аудита ИБ объектов региона.
7. Подготовка к проведению комплексного аудита ИБ объектов региона.
8. Непосредственное проведению комплексного аудита ИБ объектов региона.
9. Оформление результатов проведения комплексного аудита ИБ объектов региона.
10. Основные направления проведения комплексного аудита ИБ объектов региона (общая характеристика).
11. Аттестация объектов информатизации по требованиям ИБ как направление комплексного аудита ИБ объектов региона.
12. Контроль защищенности информации ограниченного доступа как направление комплексного аудита ИБ объектов региона.
13. Спецобследование выделенных помещений как направление комплексного аудита ИБ объектов региона.
14. Спецобследование объектов вычислительной техники как направление комплексного аудита ИБ объектов региона.

15. Проектирование объектов в защищенном исполнении как направление комплексного аудита ИБ объектов региона.

16. Поставка, установка и наладка технических средств обработки и защиты информации как направление комплексного аудита ИБ объектов региона.

17. Организация комплексного аудита ИБ объектов региона.

18. Технические средства и системы комплексного аудита ИБ объектов региона.

19. Концептуальная модель комплексного аудита ИБ объектов региона.

20. Подготовка специалистов-аудиторов по комплексному аудиту ИБ объектов региона.

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

Формой контроля знаний по дисциплине «Информационная безопасность финансово-кредитных структур» 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 образовательного процесса	тестирование	ПК-1 ПК-2	20 вопросов	Компьютерное тестирование ; время отведенное на процедуру - 30 минут	Результаты тестирования предоставляются в день проведения процедуры	***Преподаватель указывает критерии оценки данного вида контроля. Например, критерии оценки определяются процентным соотношением. Неявка – 0. Неудовлетворительно – менее 50% правильных ответов Удовлетворительно - от 51% правильных***

						ответов. Хорошо - от 70%. Отлично – от 90%
Проводится в сроки, установленные графиком образовательного процесса	тестирование	ПК-1 ПК-2	20 вопросов	Компьютерное тестирование; время отведенное на процедуру – 30 минут	Результаты тестирования предоставляются в день проведения процедуры	***Преподаватель указывает критерии оценки данного вида контроля. Например, критерии оценки определяются процентным соотношением. Неявка – 0. Неудовлетворительно – менее 50% правильных ответов Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%***
Проводится в сроки, установленные графиком образовательного процесса	Зачет	ПК-1 ПК-2	3 вопроса	Зачет проводится в письменной форме, путем ответа на вопросы. Время, отведенное на процедуру – 30 минут.	Результаты предоставляются в день проведения зачета	***Критерии оценки:*** ***«Зачтено»:*** ***знание основных понятий предмета;*** ***умение использовать и применять полученные знания на практике;*** ***работа на семинарских занятиях;*** ***знание основных научных теорий, изучаемых предметов;*** ***ответ на вопросы билета.*** ***«Не зачтено»:*** ***демонстрирует частичные знания по темам дисциплин;*** ***незнание основных понятий***

						предмета; неумение использовать и применять полученные знания на практике; не работал на семинарских занятиях; не отвечает на вопросы.

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.

Типовые вопросы, выносимые на тестирование

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

1. Аудит информационной безопасности – это:

   оценка текущего состояния системы информационной безопасности

   проверка используемых компанией информационных систем, систем безопасности

   это проверка способности успешно противостоять угрозам

   специальная проверка соответствия организации и эффективности защиты информации установленным требованиям и/или нормам

2. Анализ рисков включает в себя:

   набор адекватных контрмер осуществляется в ходе управления рисками

   анализ причинения ущерба и величины ущерба, наносимого ресурсам ИС, в случае осуществления угрозы безопасности

   выявление существующих рисков и оценку их величины

мероприятия по обследованию безопасности ИС, с целью определения того какие ресурсы и от каких угроз надо защищать, а также в какой степени те или иные ресурсы нуждаются в защите

3. Активный аудит – это:

   исследование средств для определения соответствия их решениям задач информационной безопасности

   исследование состояние системы сетевой защиты, использование которой помогает хакеру проникнуть в сети и нанести урон компании

   исследование состояния защищенности информационной системы с точки зрения хакера (или некоего злоумышленника, обладающего высокой квалификацией в области информационных технологий).

4. В число граней, позволяющих структурировать средства достижения информационной безопасности, входят:
   меры обеспечения целостности
   административные меры
   меры административного воздействия

5. Дублирование сообщений является угрозой:
   доступности
   конфиденциальности
   целостности

6. Самыми опасными источниками внутренних угроз являются:
   некомпетентные руководители
   обиженные сотрудники
   любопытные администраторы

7. Для внедрения бомб чаще всего используются ошибки типа:
   отсутствие проверок кодов возврата
   переполнение буфера
   нарушение целостности транзакций

8. В число целей политики безопасности верхнего уровня входят:
   решение сформировать или пересмотреть комплексную программу безопасности
   обеспечение базы для соблюдения законов и правил +
   обеспечение конфиденциальности почтовых сообщений

9. В число целей программы безопасности верхнего уровня входят:
   управление рисками

определение ответственных за информационные сервисы
определение мер наказания за нарушения политики безопасности

10. В рамках программы безопасности нижнего уровня осуществляются:
стратегическое планирование
повседневное администрирование
отслеживание слабых мест защиты

11. Политика безопасности строится на основе:
общих представлений об ИС организации
изучения политик родственных организаций
анализа рисков

12. В число целей политики безопасности верхнего уровня входят:
формулировка административных решений по важнейшим аспектам реализации программы безопасности
выбор методов аутентификации пользователей
обеспечение базы для соблюдения законов и правил

Типовые вопросы, выносимые на зачет

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 инфомационная 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 (дилинга).

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»
21. Информационная безопасность модели Интернет - банкинга.
22. Информационная безопасность расчетов банковскими картами в Интернете.
23. Место ЭЦП в ряду криптографических механизмов. История возникновения ЭЦП в России. Общее правило создания ЭЦП. Общее правило верификации ЭЦП.
24. Схема защищенного информационного обмена при использовании симметричных методов защиты информации.
25. Схема защищенного информационного обмена при использовании криптографических алгоритмов с открытыми ключами.
26. Применение и информационная безопасность режима электронной кодовой книги. Режима сцепления блоков шифротекста. Режима обратной связи по шифротексту.
27. Режим счетчика (counter). Функция хеширования и асиметричные алгоритмы.
28. Информационная безопасность и защита электронных транзакций протокол (SSL). Схема работы протокола SET.
29. Информационная безопасность электронных платежей с помощью цифровых денег.
30. Информационная безопасность расчетной функции банков и ее автоматизации. Схема обработки платежного документа клиентами.
31. Информационная безопасность и ключевые принципы для системно – значимых платежных систем. Определение количества ресурсов, которые банк будет держать на своих корсчетах.
32. Информационная безопасность и правила обмена электронными документами. Общие требования, предъявляемые к ЭД (пакетам ЭД).

33. Информационная безопасность при составление и направление ЭД участником – отправителем.

34. Информационная безопасность и порядок контроля ЭД, полученных от участников – отправителей. Порядок оформления ЭД, подтверждающих исполнение ЭД участников.

35. Информационная безопасность и порядок приема к исполнению ЭД участником – получателем. Порядок хранения и уничтожения ЭД.

Приложение 2

Методические указания для обучающихся по освоению дисциплины (модуля)

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ФИНАНСОВО-КРЕДИТНЫХ СТРУКТУР

Направление подготовки: 10.04.01 - Информационная безопасность

Направленность (профиль): Менеджмент информационной безопасности

Уровень высшего образования: магистратура

Форма обучения: очная

Королев
2023

1. Общие положения

Цели дисциплины:

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 необходимых 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.

Задачи дисциплины:

- Теоретические основы подготовки студентов в области Информационной безопасности кредитно-финансовых структур
- Практические аспекты формирования подходов к выполнению самостоятельных исследований студентами в области информационная безопасности кредитно-финансовых структур.

2. Указания по проведению практических (семинарских) занятий

Тема 1. Техническая платформа банковских информационных систем региона. Состав автоматизированных рабочих мест и их взаимосвязь в банковской информационной системе

Практическое занятие 1

Вид практического занятия**:** *подготовка доклада.*

Образовательные технологии: *групповая дискуссия.*

Использование интерактивных методов обучения: метод проектов, учебные тренинги (метод упражнений, метод разбора конкретных ситуаций)

Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Информационные технологии управления КБ и иные технологии оказания КБ услуг.
2. Состав и свойства информационных объектов системы бюджетирования.
3. Функциональность и алгоритмы системы бюджетирования.
4. Требования к системы бюджетирования для быстрого внедрения. Услуги и операции кредитного учреждения.

Продолжительность занятия -3 ч.

Тема 2. Технологии сбора и хранения данных — концепция информационных хранилищ в органах государственной власти и местного самоуправления региона (финансово-кредитная сфера)

Практическое занятие 2

Вид практического занятия**:** *подготовка доклада.*

Образовательные технологии: *беседа*

Использование интерактивных методов обучения: метод проектов, учебные тренинги (метод упражнений, метод разбора конкретных ситуаций)

Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Технологии извлечения, преобразования и загрузки данных.
2. Концепции организации хранения данных.
3. База метаданных информационного хранилища (репозиторий ИХ).
4. Метаданные, относящиеся к пользователям и администраторам ИХ и ИАС.
5. Содержание и назначение таблицы фактов.
6. Таблицы размерности (измерений), другие компоненты модели.
7. Схемы представления многомерных данных.

Продолжительность занятия -3 ч.

Тема 3. Признаки OLAP-систем, технологии оперативного и интеллектуального анализа данных в органах государственной власти и местного самоуправления региона

Практическое занятие 3

Вид практического занятия**:** *подготовка доклада.*

Образовательные технологии: *практическая работа в группах.*

Использование интерактивных методов обучения: метод проектов, учебные тренинги (метод упражнений, метод разбора конкретных ситуаций)

Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Подходы к выполнению анализа средствами информационных технологий (IT-анализа)
2. Классификация IT-анализа по режиму и темпу
3. Требования, предъявляемые к OLAP-системам
4. Задачи и содержание оперативного (OLAP) анализа.
5. Типы многомерных OLAP-систем.
6. Интеллектуальный анализ данных Data mining.
7. Содержание понятия знания. Классификация видов знаний.
8. Задачи Data mining.
9. Специфические методы и области применения data mininga.

Продолжительность занятия -3 ч.

Тема 4. Содержание и методы анализа и прогнозирования бизнес-процессов в кредитно – финансовых организациях региона

Практическое занятие 4

Вид практического занятия**:** *подготовка реферата.*

Образовательные технологии: *беседа.*

Использование интерактивных методов обучения: метод проектов, учебные тренинги (метод упражнений, метод разбора конкретных ситуаций)

Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Содержание экономического анализа.
2. Классификация методов анализа.
3. Аннотация содержания методов анализа в экономической предметной области.
4. Методики проведения анализа в маркетинговой деятельности.
5. Анализ обеспечения ресурсами.
6. Анализ в области логистики.
7. Финансовый анализ.
8. Анализ инвестиций и инноваций.

9. Методы стратегического анализа.
10. Анализ стратегической позиции предприятия.
11. Анализ ситуации по слабым сигналам и оценка рисков.
12. Анализ отклонений.
13. Анализ полей бизнеса.
14. Информационный обмен, связанный с аналитической работой в кредитно – финансовой деятельности .

Продолжительность занятия -3 ч.

Тема 5. Основы создания и применения информационно-аналитических систем информационной безопасности в кредитно – финансовой сфере региона
Практическое занятие 5

Вид практического занятия**:** *подготовка доклада.*
Образовательные технологии: *групповая дискуссия.*

Использование интерактивных методов обучения: метод проектов, учебные тренинги (метод упражнений, метод разбора конкретных ситуаций)

Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Программные инструментальные средства ИАС.
2. Состав программных инструментальных средств ИАС.
3. Средства сбора и доработки данных.
4. Средства преобразования данных.
5. Средства оперативного (OLAP) анализа.
6. Средства интеллектуального анализа данных.
7. Управление и проектирование ИАС.
8. Управление информационно-аналитическими системами.
9. Задачи и средства администрирования ИАС.
10. Принципы проектирования информационных хранилищ ИАС.
11. Рынок инструментальных средств ИАС.

Продолжительность занятия -3 ч.

3. Указания по проведению лабораторного практикума

Цель и задачи выполнения лабораторных работ: Определение порядка и последовательности действий по обоснованию предложений руководителю по результатам анализа и прогноза по заданной ситуации.

Методика *определяется моделью соответствующей задачи, решаемой обучающимся на занятии по заданию преподавателя)* и средства *для* выполнения лабораторных работ: общее *программное обеспечение*

Этапы выполнения лабораторных работ *(Постановка задачи лабораторной работы. Ознакомление обучающегося с содержанием и объемом лабораторной работы. Порядок выполнения лабораторной работы. Регистрация результатов и оформление отчета о лабораторной работе. Заключительная часть лабораторной работы).*

Тематика лабораторных работ и задания к ним *(тематика лабораторных работ должна соответствовать рабочей программе дисциплины).*

Лабораторная работа № 1.
Тема: Структура информационных ресурсов и администрирование в компьютерных системах
Цель занятия: Определение конфигурации информационных ресурсов компьютерных систем. Администрирование в компьютерных системах.
Продолжительность практического занятия- 2 часа
Задание.

Агропромышленная фирма «Юниор» имеет головное предприятие в Москве и несколько дочерних фирм в различных регионах России. К руководству фирмы «Юниор» на одной специализированной выставке обратился господин N, представившийся сотрудником известной зарубежной компании «ABC», с предложением об участии в совместном проекте в регионе, в котором «Юниор» имеет дочернюю фирму.

ВОПРОСЫ:

- 1. Какие мероприятия по проверке потенциального зарубежного партнера компании «ABC» должна провести Служба Конкурентной Разведки фирмы «Юниор»?
- 2. На какие моменты необходимо обратить особое внимание?

Лабораторная работа № 2. Анализ угроз информационной безопасности
Цель занятия: Факторы, воздействующие на защищаемую информацию. Классификация угроз. Естественные и искусственные угрозы. Основные направления и методы реализации угроз.
Основные виды атак на КС, их классификация. Проблемы обеспечения информационной безопасности в проводных КС.
Беспроводной доступ к локальным сетям. Угрозы и уязвимости в беспроводных компьютерных системах.
Продолжительность практического занятия-2 часа
Задание.

Фармацевтическая компания «Иванов и сын» разработала и запатентовала уникальный лекарственный препарат. Важнейшим компонентом этого препарата является сырье, ввозимое из-за рубежа (в мире имеется всего несколько поставщиков этого сырья). Руководство компании планирует выйти на рынок лекарственных препаратов аналогичного класса и поручает службе безопасности провести анализ конкурентной среды.

ВОПРОСЫ:

- 1. Какой метод анализа следует применить для решения этой задачи?
- 2. Предложить методику проведения анализа. Какая, на ваш взгляд, наиболее опасная внешняя угроза существует для этой фирмы?

Лабораторная работа № 3. Основные уровни защиты информации в компьютерных системах
Цель занятия: Методы и средства обеспечения защиты информации в компьютерных системах. Защита представления информации. Защита содержания информации.

Сертификация программных и программно-технических средств защиты конфиденциальной компьютерной информации.
Методы обеспечения защиты информации – препятствие, маскировка, управление доступом. Функции защиты при управлении доступом. Принуждение и побуждение.
Физические средства защиты компьютерных систем. Нейтрализация утечки информации по электромагнитным каналам – применение генераторов шума. Защита от наводок. Аппаратные средства защиты в КС. Задачи, решаемые программными средствами защиты.
Продолжительность практического занятия-2 часа
Задание.

Российская транспортная компания «Зевс» осуществляет грузоперевозки элементов мебели (мебельный щит, гнутые детали и т.д.) на мебельные фабрики конкурирующих фирм «Альт» (Германия) и «Вист» (Италия). Представители фирмы «Альт» пытаются получить конфиденциальную информацию у служащих фирмы «Зевс» об объемах поставок фирмы «Вист», графике движений, реквизитах грузов, стоимости транспортных услуг и т.д.

ВОПРОСЫ:

1. Какими методами компания «Альт» может получить необходимую ей конфиденциальную информацию?

2.Какие меры должна предпринять компания «Вист» для защиты собственной конфиденциальной информации?

Лабораторная работа № 4. Основные положения формальной теории защиты информации
Цель занятия: Концепция монитора безопасности обращений в КС.
Правила разграничения доступа субъектов к объектам в ОС.
Монитор безопасности обращений (МБО) субъектов к объектам. Схема монитора безопасности обращений. Функции МБО. Свойства МБО
Продолжительность практического занятия-2 часа
Задание.

Малое предприятие «Электрон», занимающееся разработкой программных продуктов, успешно конкурирует с зарубежной фирмой «Гейтсан». Успех «Электрона» во многом связан с группой (из 3 человек) высококвалифицированных программистов.

ВОПРОСЫ:

- 1. Какие шаги может предпринять фирма «Гейтсан» для вытеснения фирмы «Электрон» с рынка?
- 2. Какие индикаторы (внешние проявления) могут служить сигналами о начале наступления «Гейтсана»?
- 3. На что должны быть направлены действия Службы Конкурентной Разведки фирмы «Электрон» для защиты интересов своей фирмы?

4. Указания по проведению самостоятельной работы студентов

№ п/п	Наименование блока (раздела) дисциплины	Виды СРС
1.	Техническая платформа банковских информационных систем региона. Состав автоматизированных рабочих мест и их взаимосвязь в банковской информационной системе	***Подготовка докладов и презентаций по темам:*** Нормативно-методологические основы комплексного аудита информационной безопасности. Базовые положения по комплексному аудиту информационной безопасности предприятий (учреждений, организаций) региона. Привлекаемые силы к проведению комплексного аудита ИБ объектов региона. *Подготовка рефератов, письменная работа, самостоятельное изучение тем.*
2.	Технологии сбора и хранения данных — концепция информационных хранилищ в органах государственной власти и местного самоуправления региона (финансово-кредитная сфера)	***Подготовка докладов и презентаций по темам:*** Принципы организации и методы проведения комплексного аудита ИБ. Содержание комплексного аудита ИБ для выделенных помещений. Основные этапы комплексного аудита ИБ объектов региона. *Подготовка рефератов, письменная работа, самостоятельное изучение тем.*
3	Признаки OLAP-систем, технологии оперативного и интеллектуального анализа данных в органах государственной власти и местного самоуправления региона	***Подготовка докладов и презентаций по темам:*** Оформление результатов проведения комплексного аудита ИБ объектов региона. Основные направления проведения комплексного аудита ИБ объектов региона (общая характеристика). Аттестация объектов информатизации по требованиям ИБ как направление комплексного аудита ИБ объектов региона. *Подготовка рефератов, письменная работа, самостоятельное изучение тем.*
4	Основы создания и применения информационно-аналитических систем информационной безопасности в кредитно – финансовой сфере региона	***Подготовка докладов и презентаций по темам:*** Технические средства и системы комплексного аудита ИБ объектов региона. Концептуальная модель комплексного аудита ИБ объектов региона. Подготовка специалистов-аудиторов по комплексному аудиту ИБ объектов региона. *Подготовка рефератов, письменная работа, самостоятельное изучение тем.*

5. Указания по проведению контрольных работ для обучающихся очной формы обучения

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, сформулированных 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 в соответствии 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 – **…** страниц формата А4, напечатанного с одной стороны текста (1,5 интервал, шрифт Times New Roman).

6.Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

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», необходимых для освоения дисциплины (модуля)

Интернет-ресурсы:

3. **http://eup.ru/catalog/all-all.asp – научно-образовательный портал.**
4. **http://informika.ru/ – образовательный портал.**
3. **http://www.academy.it.ru/ – академия АЙТИ.**

7. 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.