

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Макаренко Елена Николаевна

Должность: Ректор

Дата подписания: 09.09.2024 15:43:13

Уникальный программный ключ:

c098bc0c1041cb2a4cf926cf171d6715d99abaed0ba0c8e27b35cbe1e2dbd7c78

Министерство науки и высшего образования Российской Федерации  
Федеральное государственное бюджетное образовательное  
учреждение высшего образования «Ростовский государственный  
экономический университет (РИНХ)»

УТВЕРЖДАЮ  
Директор Института  
магистратуры  
Иванова Е.А.  
«03» июня 2024г.

**Рабочая программа дисциплины  
Кибербезопасность в сфере финансов**

Направление 38.04.08 Финансы и кредит  
магистерская программа 38.04.08.05 "Финансовые инновации в  
экономике и бизнесе"

Для набора 2024 года

Квалификация  
Магистр

**КАФЕДРА            Информационная безопасность****Распределение часов дисциплины по курсам**

Курс	1		Итого	
	уп	рп		
Лекции	2	2	2	2
Практические	4	4	4	4
Итого ауд.	6	6	6	6
Контактная работа	6	6	6	6
Сам. работа	26	26	26	26
Часы на контроль	4	4	4	4
Итого	36	36	36	36

**ОСНОВАНИЕ**

Учебный план утвержден учёным советом вуза от 26.03.2024 протокол № 13.

Программу составил(и): доцент, Назарян С.А.

Зав. кафедрой: к.э.н., Радченко Ю.В.

Методическим советом направления: д.э.н., проф., Иванова О.Б.

### 1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1	Знание основ кибербезопасности для решения задач профессиональной деятельности, умение защитить компьютерную информацию от несанкционированного разглашения, обеспечивать правовую защиту компьютерной информации в профессиональной деятельности; способностью сознавать опасности и угрозы, возникающие в развитии современного информационного общества.
-----	---

### 2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

**ОПК-2:Способен применять продвинутые инструментальные методы экономического и финансового анализа в прикладных и (или) фундаментальных исследованиях в области финансовых отношений, в том числе с использованием интеллектуальных информационно-аналитических систем;**

#### В результате освоения дисциплины обучающийся должен:

<b>Знать:</b>
информационные технологии, правовые базы данных, требования информационной безопасности (соотнесено с индикатором ОПК-2.1)
<b>Уметь:</b>
решать стандартные задачи профессиональной деятельности с применением информационных технологий и учетом основных требований информационной безопасности (соотнесено с индикатором ОПК-2.2)
<b>Владеть:</b>
информационными технологиями и правовыми базами данных для решения задач профессиональной деятельности с учетом требований информационной безопасности (соотнесено с индикатором ОПК-2.3)

### 3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

#### Раздел 1. Общие вопросы информационной безопасности

№	Наименование темы / Вид занятия	Сем естр	Часо в	Компетен -	Литература
1.1	Тема 1 «Введение в информационную безопасность". Понятие информации, защиты информации, информационной системы, информационной безопасности. Цель защиты информации. Базовые свойства информации: конфиденциальность, целостность, доступность. / Лек /	1	2	ОПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4
1.2	Тема 1 «Введение в информационную безопасность". Нормативно-правовая база функционирования систем защиты информации. Российское законодательство по защите информационных технологий. Правовая защита программного обеспечения авторским правом. Компьютерные преступления и особенности их расследования с использованием текстового редактора LibreOffice. / Пр /	1	2	ОПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4
1.3	Тема 1 "Введение в информационную безопасность". Правовая защита информации. / Ср /	1	2	ОПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4
1.4	Тема 2 «Санкционированный и несанкционированный доступ». Понятие доступа к информации, субъекта и объекта доступа, санкционированного и несанкционированного доступа, нарушителя. Неформальная модель нарушителя. Причины несанкционированного доступа к информации. Последствия несанкционированного доступа к информации. / Ср /	1	2	ОПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4
1.5	Тема 2 «Санкционированный и несанкционированный доступ». Несанкционированный доступ к информации	1	2	ОПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1,

	(НСД). Идентификация. Аутентификация. Выбор паролей с использованием текстового редактора LibreOffice. / Пр /				Л2.2, Л2.3, Л2.4
1.6	Тема 2 «Санкционированный и несанкционированный доступ». Административная защита информации. / Ср /	1	4	ОПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4
<b>Раздел 2. Технологии организации работы с информацией</b>					
№	Наименование темы / Вид занятия	Семестр	Часы	Компетенции	Литература
2.1	Тема 3 «Понятие угрозы, уязвимости, риска». Понятие угрозы, классификация угроз. Понятие уязвимости, атаки на компьютерную систему. Понятие риска. Виды утечки информации в юриспруденции. Понятие канала утечки информации, основные каналы утечки информации. Классификация злоумышленников. / Ср /	1	2	ОПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4
2.2	Тема 3 «Понятие угрозы, уязвимости, риска». Технологии организации работы с информацией. Поиск, сохранение информации, проверка на вирусы. / Ср /	1	2	ОПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4
2.3	Тема 3 «Понятие угрозы, уязвимости, риска». Уязвимость компьютерных систем. / Ср /	1	2	ОПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4
2.4	Тема 4 «Парольные системы идентификации и аутентификации пользователей». Особенности парольных систем, основные типы угроз безопасности парольных систем. Требования к выбору и использованию паролей. / Ср /	1	2	ОПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4
2.5	Тема 4 «Парольные системы идентификации и аутентификации пользователей». Архиваторы. Архивы. Методы сжатия архиваторов. Сегментирование. Возможности ОС по созданию учетной записи пользователя с ограниченными правами. Порядок удаления ограниченной учетной записи. / Ср /	1	2	ОПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4
2.6	Тема 5 «Парольные системы идентификации и аутентификации пользователей». Защита электронной почты. / Ср /	1	8	ОПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4
2.7	/ Зачёт /	1	4	ОПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4

#### 4. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Структура и содержание фонда оценочных средств для проведения текущей и промежуточной аттестации представлены в Приложении 1 к рабочей программе дисциплины.

#### 5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

##### 5.1. Основная литература

	Авторы,	Заглавие	Издательство, год	Колич-во
Л1.1	Руденков Н. А., Пролетарский А. В., Смирнова Е. В., Суоров А. М.	Технологии защиты информации в компьютерных сетях: учебное пособие	Москва: Национальный Открытый Университет «ИНТУИТ», 2016	<a href="https://biblioclub.ru/index.php?page=book&amp;id=428820">https://biblioclub.ru/index.php?page=book&amp;id=428820</a> неограниченный доступ для зарегистрированных пользователей

	Авторы,	Заглавие	Издательство, год	Колич-во
Л1.2	Ковалев Д. В., Богданова Е. А.	Информационная безопасность: учебное пособие	Ростов-на-Дону: Южный федеральный университет, 2016	<a href="https://biblioclub.ru/index.php?page=book&amp;id=493175">https://biblioclub.ru/ index.php? page=book&amp;id=493 175</a> неограниченный доступ для зарегистрированны х пользователей
Л1.3	Шилов, А. К.	Управление информационной безопасностью: учебное пособие	Ростов-на-Дону, Таганрог: Издательство Южного федерального университета, 2018	<a href="https://www.iprbookshop.ru/87643.html">https:// www.iprbookshop.ru/ 87643.html</a> неограниченный доступ для зарегистрированны х пользователей
Л1.4	Шаньгин, В. Ф.	Информационная безопасность и защита информации	Саратов: Профобразование, 2019	<a href="https://www.iprbookshop.ru/87995.html">https:// www.iprbookshop.ru/ 87995.html</a> неограниченный доступ для зарегистрированны х пользователей
Л1.5	Артемов, А. В.	Информационная безопасность: курс лекций	Орел: Межрегиональная Академия безопасности и выживания (МАБИБ), 2014	<a href="https://www.iprbookshop.ru/33430.html">https:// www.iprbookshop.ru/ 33430.html</a> неограниченный доступ для зарегистрированны х пользователей

### 5.2. Дополнительная литература

	Авторы,	Заглавие	Издательство, год	Колич-во
Л2.1		Вестник Института законодательства и правовой информации имени М.М. Сперанского: журнал	Иркутск: Институт законодательства и правовой информации, 2017	<a href="https://biblioclub.ru/index.php?page=book&amp;id=457912">https://biblioclub.ru/ index.php? page=book&amp;id=457 912</a> неограниченный доступ для зарегистрированны х пользователей
Л2.2	Катанова, Т. Н., Галкина, Л. С., Жданов, Р. А.	Информационная безопасность: лабораторный практикум	Пермь: Пермский государственный гуманитарно- педагогический университет, 2018	<a href="https://www.iprbookshop.ru/86357.html">https:// www.iprbookshop.ru/ 86357.html</a> неограниченный доступ для зарегистрированны х пользователей
Л2.3		БИТ. Бизнес & Информационные технологии: журнал	Москва: Положевец и партнеры, 2019	<a href="https://biblioclub.ru/index.php?page=book&amp;id=562409">https://biblioclub.ru/ index.php? page=book&amp;id=562 409</a> неограниченный доступ для зарегистрированны х пользователей
Л2.4	Суворова, Г. М.	Информационная безопасность: учебное пособие	Саратов: Вузовское образование, 2019	<a href="https://www.iprbookshop.ru/86938.html">https:// www.iprbookshop.ru/ 86938.html</a> неограниченный доступ для зарегистрированны х пользователей

### 5.3 Профессиональные базы данных и информационные справочные системы

Справочная правовая система "Консультант Плюс"

Russian Science Citation Index (RSCI)clarivate.ru

zbMATH zbmath.org

### 5.4. Перечень программного обеспечения

LibreOffice

**5.5. Учебно-методические материалы для студентов с ограниченными возможностями**

При необходимости по заявлению обучающегося с ограниченными возможностями здоровья учебно-методические материалы предоставляются в формах, адаптированных к ограничениям здоровья и восприятия информации. Для лиц с нарушениями зрения: в форме аудиофайла; в печатной форме увеличенным шрифтом. Для лиц с нарушениями слуха: в форме электронного документа; в печатной форме. Для лиц с нарушениями опорно-двигательного аппарата: в форме электронного документа; в печатной форме.

**6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)**

Помещения для всех видов работ, предусмотренных учебным планом, укомплектованы необходимой специализированной учебной мебелью и техническими средствами обучения:

- столы, стулья;

- персональный компьютер / ноутбук (переносной);

- проектор, экран / интерактивная доска.

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

Методические указания по освоению дисциплины представлены в Приложении 2 к рабочей программе дисциплины.

## ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

### 1 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

#### 1.1 Показатели и критерии оценивания компетенций:

ЗУН, составляющие компетенцию	Показатели оценивания	Критерии оценивания	Средства оценивания
<b>ОПК-2: Способен применять продвинутые инструментальные методы экономического и финансового анализа в прикладных и(или) фундаментальных исследованиях в области финансовых отношений, в том числе с использованием интеллектуальных информационно-аналитических систем</b>			
З: информационные технологии, правовые базы данных, требования информационной безопасности (соотнесено с индикатором ОПК-2.1)	изучает методы защиты информации и применения их в профессиональных целях, а также при подготовке к зачету	полнота и обоснованность выбора методов защиты информации на основе изученной литературы	З (1-44) УО (Раздел 1 вопросы 1-26, Раздел 2 вопросы 8-11, 19-21)
У: решать стандартные задачи профессиональной деятельности с применением информационных технологий и учетом основных требований информационной безопасности (соотнесено с индикатором ОПК-2.2)	обеспечивает правовую защиту компьютерной информации в профессиональной деятельности при выполнении практико-ориентированных и практических заданий	правильность применения методов системного подхода для решения практико-ориентированных и практических заданий	ПЗ (1.1, 1.2, 2.1) ПОЗЗ (1-5)
В: информационными технологиями и правовыми базами данных для решения задач профессиональной деятельности с учетом требований информационной	решение практико-ориентированных и практических заданий: применяет разные подходы защиты экономических данных средствами LibreOffice	полнота и обоснованность выбора методов защиты для решения практико-ориентированных и практических заданий	ПЗ (1.1, 1.2, 2.1) ПОЗЗ (1-5)

безопасности (соотнесено с индикатором ОПК-2.3)			
--	--	--	--

*ПЗ – практические задания, ПОЗЗ - практико-ориентированные задания к зачету, З – вопросы к зачету, УО- устный опрос*

## 1.2 Шкалы оценивания:

Текущий контроль успеваемости и промежуточная аттестация осуществляется в рамках накопительной балльно-рейтинговой системы в 100-балльной шкале:

50-100 баллов (зачет)

0-49 баллов (незачет)

## 2 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

### Вопросы к зачету по дисциплине

1. Теоретические аспекты информационной безопасности экономических систем. Основные понятия.
2. Экономическая информация как объект безопасности.
3. Государственное регулирование информационной безопасности
4. Организация системы защиты информации экономических систем.
5. Подходы, принципы, методы и средства обеспечения безопасности.
6. Организационно-техническое обеспечение компьютерной безопасности.
7. Защита от компьютерных вирусов.
8. Электронная цифровая подпись и особенности ее применения
9. Правовые основы лицензирования в области защиты информации.
10. Сущность и содержание сертификации в области защиты информации.
11. Правовые основы защиты коммерческой тайны.
12. Правовые основы защиты конфиденциальной информации.
13. Понятие доступа к информации, субъекта и объекта доступа, санкционированного и несанкционированного доступа, нарушителя.
14. Неформальная модель нарушителя.
15. Причины несанкционированного доступа к информации.
16. Последствия несанкционированного доступа к информации.
17. Понятие угрозы, классификация угроз.
18. Понятие уязвимости, атаки на компьютерную систему.
19. Понятие риска.
20. Виды утечки информации.
21. Понятие канала утечки информации, основные каналы утечки информации.
22. Классификация злоумышленников.
23. Основные подходы к построению моделей защиты информационных систем, основанные на понятии ценности информации.
24. Особенности парольных систем, основные типы угроз безопасности парольных систем.
25. Требования к выбору и использованию паролей.
26. Защита электронной почты.
27. Понятие криптографии, шифрования и дешифрования, ключа шифрования, шифротекста, криптоалгоритма.
28. Классификация криптосистем.
29. Процесс шифрования текста с помощью таблицы Вижинера.
30. Расшифровка текста с помощью таблицы Вижинера.
31. Система шифрования Цезаря.
32. Шифры перестановки.



33. Обеспечение информационной безопасности автоматизированных бухгалтерских систем
34. Обеспечение информационной безопасности консалтинговых систем.
35. Информационная безопасность электронной коммерции
36. Понятие криптоанализа, криптоаналитической атаки.
37. Основные типы криптоаналитических атак, криптостойкость шифра.
38. Требования к шифрам, используемым для криптографической защиты информации.
39. Особенности использования вычислительной техники в криптографии.
40. Принципы и процедурные аспекты алгоритма электронной цифровой подписи (ЭЦП).
41. Понятие и назначение центра распределения ключей.
42. Оценка эффективности инвестиций в информационную безопасность.
43. Безопасность в интернет.
44. Безопасность хранения данных в облачных сервисах

## Типовые практико-ориентированные задания к зачету

Задание 1. Добавить пользователей в компьютер.

Задание 2. Создать учетную запись локального пользователя.

Задание 3. Изменить учетную запись локального пользователя на учетную запись администратора.

Задание 4. Выполнить настройку учетной записи с ограниченными правами.

Задание 5. Выполнить добавление учетных записей, используемых приложениями.

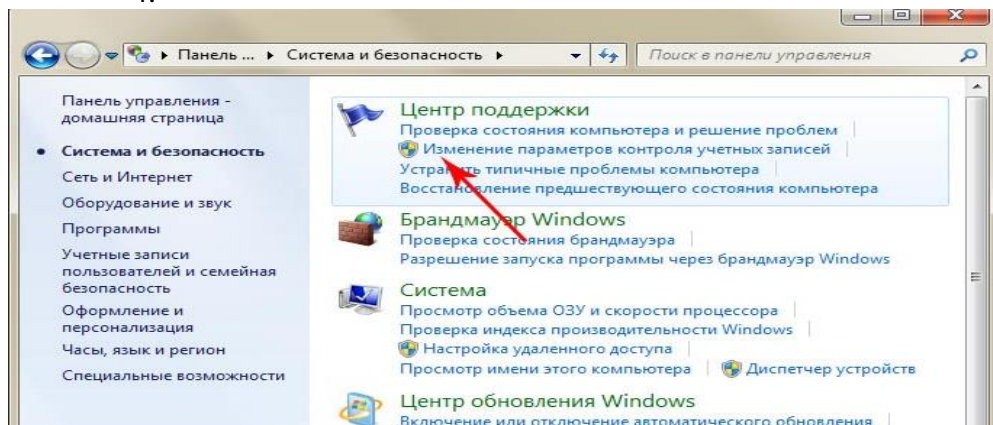
## Ключ для контроля правильности выполнения практико-ориентированные задания к зачету

1. Добавление пользователей в рабочий или учебный компьютер. Выберите параметры > "Пуск" > "Учетные записи > Другие пользователи". В разделе "Рабочие или учебные > добавить рабочую или учебную учетную запись" выберите "Добавить учетную запись". Введите учетную запись этого пользователя, выберите тип учетной записи и нажмите Добавить.

2. Создание учетной записи локального пользователя. Выберите Пуск > Параметры > Учетные записи, а затем Семья и другие пользователи. Рядом с пунктом Добавить другого пользователя выберите Добавить учетную запись. Выберите пункт У меня нет учетных данных этого пользователя и на следующей странице нажмите Добавить пользователя без учетной записи Майкрософт. Введите имя пользователя, пароль, подсказку о пароле или выберите секретные вопросы, а затем нажмите Далее.

3. Изменение учетной записи локального пользователя на учетную запись администратора. Выберите Пуск > Параметры > Учетные записи. В разделе Семья и другие пользователи щелкните имя владельца учетной записи (под ним должно быть указано "Локальная учетная запись") и выберите Изменить тип учетной записи. В разделе Тип учетной записи выберите Администратор, и нажмите ОК. Войдите в систему с новой учетной записью администратора.

4.



5.Добавление на компьютер учетной записи, используемой приложениями: Выберите **параметры** > параметров > **учетных записей** > **электронной почты & учетных записей**. Добавление учетной записи, используемой по электронной почте. выберите "Добавить учетную запись" в разделе "Учетные записи", используемые электронной почтой, **календарем и контактами**. Для других приложений выберите "Добавить учетную запись Майкрософт" или "Добавить рабочую или учебную учетную запись". Следуйте инструкциям по добавлению учетной записи.

### **Критерии оценивания:**

– 50-100 баллов (зачет) – изложенный материал фактически верен, наличие глубоких исчерпывающих знаний; правильные, уверенные действия по применению полученных знаний на практике, грамотное и логически стройное изложение материала при ответе; практико-ориентированное задание выполнено правильно и прокомментировано; наличие твердых и достаточно полных знаний, правильные действия по применению знаний на практике, четкое изложение материала, допускаются отдельные логические и стилистические погрешности, неуверенность и неточность ответов на дополнительные и наводящие вопросы; практико-ориентированное задание выполнено правильно, но не прокомментировано; при неполном ответе на вопросы; затрудняется ответить на дополнительные вопросы; практико-ориентированное задание выполнено с ошибками и отсутствуют комментарии;

– 0-49 баллов (незачет) – ответы не связаны с вопросами, наличие грубых ошибок в ответе, непонимание сущности излагаемого вопроса, неумение применять знания на практике, неуверенность и неточность ответов на дополнительные и наводящие вопросы; практико-ориентированное задание не выполнено.

–

## **Практические задания**

### **1. Тематика заданий по разделам и темам**

#### **Раздел 1 «Организация системы защиты информации экономических данных»**

Практическое задание 1.1 (10 баллов). Организация защиты документов средствами пакета LibreOffice.

Практическое задание 1.2 (20 баллов). «Парольные системы идентификации и аутентификации пользователей». Архиваторы. Архивы. Методы сжатия архиваторов. Сегментирование. Возможности ОС по созданию учетной записи пользователя с ограниченными правами. Порядок удаления ограниченной учетной записи.

#### **Раздел 2 «Методы и средства защиты данных в системе бухгалтерского учета».**

Практическое задание 2.1 (20 баллов). «Принципы криптографической защиты информации». Процесс шифрования текста с помощью таблицы Вижинера. Расшифровка текста с помощью таблицы Вижинера. Система шифрования Цезаря. Шифры перестановки

Практическое задание 2.2 (20 баллов). "Защита информации от несанкционированного доступа в системе 1С" Изучение механизмов аутентификации. Настройки входа в Программу. Обеспечение защиты персональных данных

### **Критерии оценивания:**

Баллы указаны возле каждого лабораторного задания

Неправильное выполненное задание – 0 баллов

Максимальное количество баллов по лабораторным заданиям – 70

## **Перечень вопросов для устного опроса**

### **Раздел 1. Организация системы защиты информации экономических данных**

1. Теоретические аспекты информационной безопасности экономических систем. Основные понятия.
2. Экономическая информация как объект безопасности.

3. Государственное регулирование информационной безопасности
4. Организация системы защиты информации экономических систем.
5. Подходы, принципы, методы и средства обеспечения безопасности.
6. Организационно-техническое обеспечение компьютерной безопасности.
7. Защита от компьютерных вирусов.
8. Электронная цифровая подпись и особенности ее применения
9. Правовые основы лицензирования в области защиты информации.
10. Сущность и содержание сертификации в области защиты информации.
11. Правовые основы защиты коммерческой тайны.
12. Правовые основы защиты конфиденциальной информации.
13. Понятие доступа к информации, субъекта и объекта доступа, санкционированного и несанкционированного доступа, нарушителя.
14. Неформальная модель нарушителя.
15. Причины несанкционированного доступа к информации.
16. Последствия несанкционированного доступа к информации.
17. Понятие угрозы, классификация угроз.
18. Понятие уязвимости, атаки на компьютерную систему.
19. Понятие риска.
20. Виды утечки информации.
21. Понятие канала утечки информации, основные каналы утечки информации.
22. Классификация злоумышленников.
23. Основные подходы к построению моделей защиты информационных систем, основанные на понятии ценности информации.
24. Особенности парольных систем, основные типы угроз безопасности парольных систем.
25. Требования к выбору и использованию паролей.
26. Защита электронной почты.

## **Раздел 2. Методы и средства защиты данных в системе бухгалтерского учета**

1. Понятие криптографии, шифрования и дешифрования, ключа шифрования, шифротекста, криптоалгоритма.
2. Принципы функционирования криптографической системы.
3. Классификация криптосистем.
4. Процесс шифрования текста с помощью таблицы Вижинера.
5. Расшифровка текста с помощью таблицы Вижинера.
6. Система шифрования Цезаря.
7. Шифры перестановки.
8. Обеспечение информационной безопасности автоматизированных бухгалтерских систем
9. Обеспечение информационной безопасности консалтинговых систем.
10. Информационная безопасность электронной коммерции
11. Понятие криптоанализа, криптоаналитической атаки.
12. Основные типы криптоаналитических атак, криптостойкость шифра.
13. Требования к шифрам, используемым для криптографической защиты информации.
14. Особенности использования вычислительной техники в криптографии.
15. Принципы и процедурные аспекты алгоритма электронной цифровой подписи (ЭЦП).
16. Понятие и назначение центра распределения ключей.
17. Требования Диффи и Хеллмана.
18. Алгоритм шифрования RSA.
19. Оценка эффективности инвестиций в информационную безопасность.
20. Безопасность в интернет.
21. Безопасность хранения данных в облачных сервисах

### **Критерии оценивания:**

Для каждого вопроса:

- 2 балла дан полный ответ на поставленный вопрос, изложение материала при ответе – грамотное и логически стройное;

- 1 балл – в ответе на поставленный вопрос были неточности;
- 0 баллов – обучающийся не владеет материалом по заданному вопросу.

Максимальное количество баллов – 30

### **3 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций**

Процедуры оценивания включают в себя текущий контроль и промежуточную аттестацию.

**Текущий контроль** успеваемости проводится с использованием оценочных средств, представленных в п. 2 данного приложения. Результаты текущего контроля доводятся до сведения студентов до промежуточной аттестации.

Зачет проводится по расписанию промежуточной аттестации.

Количество вопросов в задании – 3 (2 теоретических вопроса и 1 практико-ориентированное задание к зачету). Проверка ответов и объявление результатов производится в день зачета. Результаты аттестации заносятся в зачетную ведомость и зачетную книжку студента. Студенты, не прошедшие промежуточную аттестацию по графику сессии, должны ликвидировать задолженность в установленном порядке

## МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Учебным планом предусмотрены следующие виды занятий:

- лекции;
- практические занятия.

В ходе лекционных занятий рассматриваются основные понятия в области информационной безопасности и защиты информации, методы обнаружения и организации противодействия атак на информационные сети, требования по защите конфиденциальной информации, даются рекомендации для самостоятельной работы и подготовке к лабораторным занятиям.

В ходе практических занятий углубляются и закрепляются знания студентов по ряду рассмотренных на лекциях вопросов, развиваются навыки решения задач по защите информационных объектов.

При подготовке к лабораторным занятиям каждый студент должен:

- изучить рекомендованную учебную литературу;
- изучить конспекты лекций;
- ознакомиться с описанием лабораторной работы;
- подготовить ответы на контрольные вопросы по изучаемой теме.

В процессе подготовки к практическим занятиям студенты могут воспользоваться консультациями преподавателя.

Вопросы, не рассмотренные на лекциях и практических занятиях, должны быть изучены студентами в ходе самостоятельной работы. Контроль самостоятельной работы студентов над учебной программой дисциплины осуществляется в ходе занятий методом устного опроса. В ходе самостоятельной работы каждый студент обязан прочитать основную и, по возможности, дополнительную литературу по изучаемой теме, дополнить конспекты лекций недостающим материалом, выписками из рекомендованных источников. Выделить непонятные термины и найти их значение в энциклопедических словарях.

Для подготовки к занятиям, текущему контролю и промежуточной аттестации студенты могут воспользоваться электронно-библиотечными системами. Также обучающиеся могут взять на дом необходимую литературу на абонементе университетской библиотеки или воспользоваться читальными залами.