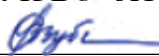


УТВЕРЖДАЮ

Заместитель директора УрСЭИ (филиал)
ОУП ВО "АТиСО" по УВР

 О.В. Зубкова

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Информационная безопасность

Направление подготовки

09.03.03 Прикладная информатика

(код и наименование направления подготовки)

Направленность (профиль)

Корпоративные информационные системы

Квалификация выпускника

Бакалавр

Кафедра: Информатики и математики

Разработчики программы:

Битехтин Денис Николаевич

Программа обсуждена на заседании кафедры Информатики и математики

Заведующий кафедрой Информатики и математики

ОГЛАВЛЕНИЕ

1. ЦЕЛЬ И ЗАДАЧИ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	3
2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	3
2.1. Планируемые результаты обучения по дисциплине	3
2.2. Результаты освоения образовательной программы	3
3. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	4
4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ) И ВИДЫ УЧЕБНОЙ РАБОТЫ	4
5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)	5
5.1. Содержание дисциплины (модуля)	5
5.2. Разделы / темы дисциплины, их трудоемкость и виды занятий	6
6. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)	7
7. ОСНОВНАЯ И ДОПОЛНИТЕЛЬНАЯ УЧЕБНАЯ ЛИТЕРАТУРА	10
8. ПЕРЕЧЕНЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ И ИНТЕРНЕТ - РЕСУРСОВ, НЕОБХОДИМЫХ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	11
9. ТРЕБОВАНИЯ К МАТЕРИАЛЬНО-ТЕХНИЧЕСКОМУ И УЧЕБНО-МЕТОДИЧЕСКОМУ ОБЕСПЕЧЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)	15
10. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ	16
11. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ	16

1. ЦЕЛЬ И ЗАДАЧИ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

Цель:

Сформировать знания о принципах опасностей и угроз, возникающих в процессе развития современного информационного общества и овладение навыками противодействия опасностям.

Задачи:

- 1.сформировать у студентов практические навыки использования различных способов правовой охраны существующих и вновь создаваемых объектов интеллектуальной собственности.
- 2.освоить основные аспекты интеграции права и информационных технологий, общих вопросов правового регулирования информационных технологий.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

2.1 Планируемые результаты обучения по дисциплине

Изучение дисциплины Информационная безопасность направлено на формирование следующих компетенций:

универсальных компетенций и индикаторов их достижения:

Категория (группа) УК	Код и наименование универсальной компетенции	Код и наименование индикатора достижений универсальной компетенции
Разработка и реализация проектов	УК-2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений.	УК-2.1. Знает необходимые для осуществления профессиональной деятельности правовые нормы.. УК-2.2. Умеет определять круг задач в рамках избранных видов профессиональной деятельности, планировать собственную деятельность исходя из имеющихся ресурсов; соотносить главное и второстепенное, решать поставленные задачи в рамках избранных видов профессиональной деятельности.. УК-2.3. Имеет практический опыт применения понятий о логике, композиции, жанре высказываний различных типов, применения нормативной базы и решения задач в области избранных видов профессиональной деятельности..
Гражданская позиция	УК-10 Способен формировать нетерпимое отношение к коррупционному поведению.	УК-10.1. Знает причины, признаки и последствия коррупционного поведения.. УК-10.2. Умеет выявлять признаки, причины и условия возникновения коррупционного поведения.. УК-10.3. Владеет методами нейтрализации коррупционного поведения..

общепрофессиональных компетенций и индикаторов их достижения:

Категория (группа) ОПК	Код и наименование универсальной компетенции	Код и наименование индикатора достижений универсальной компетенции
------------------------	--	--

Организационно-управленческие	ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	ОПК-3.1. Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.. ОПК-3.2. Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.. ОПК-3.3. Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности..
-------------------------------	--	---

2.2. Результаты освоения образовательной программы:

В результате изучения дисциплины студент должен:

Знать:

- 1.законодательство об информационных технологиях (ИТ), структуру информационного законодательства, законодательство об ИТ в системе законодательства России, понятие объектов права ИТ, понятие субъектов права ИТ.
- 2.значение информации в развитии современного информационного общества и возникающие, в связи с этим; опасности и угрозы; стандарты информационной безопасности.

Уметь:

- 1.анализировать правовую ситуацию в информационной сфере, выделяя область информационных технологий.
- 2.уметь разбираться в простейших правовых ситуациях, составлять и анализировать авторские договоры.
- 3.соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны.
- 4.ориентироваться в системе законодательства и нормативных правовых актов, регламентирующих сферу информационной безопасности.
5. использовать правовые нормы в профессиональной и общественной деятельности.

Владеть (навыки и/или опыт деятельности):

- 1.навыками анализа правовых ситуаций в области информационных технологий.
- 2.навыками составления и анализа авторских договоров и лицензий к программному обеспечению.
- 3.методами обеспечения информационной безопасности.
- 4.навыками поиска необходимых нормативных и законодательных документов.
- 5.навыками работы с нормативными и правовыми документами в профессиональной деятельности.

3. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина относится к дисциплинам обязательной части направления подготовки 09.03.03 Прикладная информатика профиль "Корпоративные информационные системы".

4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ) И ВИДЫ УЧЕБНОЙ РАБОТЫ

Объем дисциплины	Всего часов		
	Для очной формы обучения	Для очно-заочной формы обучения	Для заочной формы обучения
Общая трудоемкость дисциплины (зачетных единиц/часов)	3 / 108	0 / 0	3 / 108
Контактная работа – аудиторные занятия:	56		12
Лекции	18		4
Семинары, практические занятия	36		8
Контактная работа (зачет, экзамен, курсовая работа)	2		
Самостоятельная работа обучающегося	52		92
Промежуточная аттестация			4
Вид промежуточной аттестации	Зачет		Зачет

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Содержание дисциплины (модуля)

Тема 1. Введение в информационную безопасность.

Информационная безопасность. Основные понятия. Модели информационной безопасности. Виды защищаемой информации.

Тема 2. Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности.

Использование баз данных для нахождения и изучения нормативных документов в области информационной безопасности

Тема 3. Правовое обеспечение информационной безопасности.

Основные нормативно-правовые акты в области информационной безопасности. Правовые особенности обеспечения безопасности конфиденциальной информации и государственной тайны.

Тема 4. Использование криптографических средств защиты информации.

Создание зашифрованных файлов и криптоконтейнеров и их расшифрование.

Тема 5. Организационное обеспечение информационной безопасности.

Основные стандарты в области обеспечения информационной безопасности. Политика безопасности. Экономическая безопасность предприятия.

Тема 6. Реализация работы инфраструктуры открытых ключей.

Создание удостоверяющего центра, генерация открытых и секретных ключей, создание сертификатов открытых ключей, создание электронной подписи, проверка электронной подписи.

Тема 7. Технические средства и методы защиты информации.

Инженерная защита объектов. Защита информации от утечки по техническим каналам.

Тема 8. Средства стеганографии для защиты информации.

Использование средств стеганографии для защиты файлов.

Тема 9. Программно-аппаратные средства и методы обеспечения информационной безопасности.

Основные виды сетевых и компьютерных угроз. Средства и методы защиты от сетевых компьютерных угроз.

Тема 10. Настройка безопасного сетевого соединения.

Создание защищенного канала связи средствами виртуальной частной сети.

Тема 11. Криптографические методы защиты информации.

Симметричные и ассиметричные системы шифрования. Цифровые подписи (Электронные подписи). Инфраструктура открытых ключей. Криптографические протоколы.

Тема 12. Антивирусные средства защиты информации.

Изучение настроек средств антивирусной защиты информации.

5.2 Разделы/темы дисциплины, их трудоемкость и виды занятий

Общая трудоемкость изучения дисциплины по учебному плану: 3.Е. (часов) 3/108

Форма обучения: очная

Вид контроля: Зачет

№	Наименование темы	Всего	Лекции	Мини-ар	ци и/А	те ль на ом пе те а	(с сы
1	Тема 1. Введение в информационную безопасность.	8	1	3		4	УК-2 УК-10 ОПК-3 Л.1-7
2	Тема 2. Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности.	8	1	3		4	УК-2 УК-10 ОПК-3 Л.1-7
3	Тема 3. Правовое обеспечение информационной безопасности.	8	1	3		4	УК-2 УК-10 ОПК-3 Л.1-7
4	Тема 4. Использование криптографических средств защиты информации.	8	1	3		4	УК-2 УК-10 ОПК-3 Л.1-7
5	Тема 5. Организационное обеспечение информационной безопасности.	8	1	3		4	УК-2 УК-10 ОПК-3 Л.1-7
6	Тема 6. Реализация работы инфраструктуры открытых ключей.	8	1	3		4	УК-2 УК-10 ОПК-3 Л.1-7
7	Тема 7. Технические средства и методы защиты информации.	9	2	3		4	УК-2 УК-10 ОПК-3 Л.1-7
8	Тема 8. Средства стеганографии для защиты информации.	9	2	3		4	УК-2 УК-10 ОПК-3 Л.1-7
9	Тема 9. Программно-аппаратные средства и методы обеспечения информационной безопасности.	9	2	3		4	УК-2 УК-10 ОПК-3 Л.1-7

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

10	Тема 10. Настройка безопасного сетевого соединения.	11	2	3		6	УК-2 УК-10 ОПК-3	Л.1-7
11	Тема 11. Криптографические методы защиты информации.	9	2	3		4	УК-2 УК-10 ОПК-3	Л.1-7
12	Тема 12. Антивирусные средства защиты информации.	11	2	3		6	УК-2 УК-10 ОПК-3	Л.1-7
13	Консультации (контактная)	2			2			
14	Промежуточная аттестация (часов)							
	Всего часов	108	18	36	2	52		

Форма обучения: заочная

Вид контроля: Зачет

№	Наименование темы	Вс	е	г	о	Л	е	к	ц	и	и	м	и	н	а	р	ц	и	/	А	т	е	л	ь	н	а	б	и	т	е	р	с	ы
1	Тема 1. Введение в информационную безопасность.	8				1															7					УК-2 УК-10 ОПК-3					Л.1-7		
2	Тема 2. Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности.	8				1															7					УК-2 УК-10 ОПК-3					Л.1-7		
3	Тема 3. Правовое обеспечение информационной безопасности.	8				1															7					УК-2 УК-10 ОПК-3					Л.1-7		
4	Тема 4. Использование криптографических средств защиты информации.	8				1															7					УК-2 УК-10 ОПК-3					Л.1-7		
5	Тема 5. Организационное обеспечение информационной безопасности.	9										1									8					УК-2 УК-10 ОПК-3					Л.1-7		
6	Тема 6. Реализация работы инфраструктуры открытых ключей.	9										1									8					УК-2 УК-10 ОПК-3					Л.1-7		
7	Тема 7. Технические средства и методы защиты информации.	9										1									8					УК-2 УК-10 ОПК-3					Л.1-7		
8	Тема 8. Средства стеганографии для защиты информации.	9										1									8					УК-2 УК-10 ОПК-3					Л.1-7		
9	Тема 9. Программно-аппаратные средства и методы обеспечения информационной безопасности.	9										1									8					УК-2 УК-10 ОПК-3					Л.1-7		
10	Тема 10. Настройка безопасного сетевого соединения.	9										1									8					УК-2 УК-10 ОПК-3					Л.1-7		
11	Тема 11. Криптографические методы защиты информации.	9										1									8					УК-2 УК-10 ОПК-3					Л.1-7		
12	Тема 12. Антивирусные средства защиты информации.	9										1									8					УК-2 УК-10 ОПК-3					Л.1-7		
13	Консультации (контактная)																																
14	Промежуточная аттестация (часов)	4																	4														
	Всего часов	108				4						8							4		92												

6. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Самостоятельная работа включает следующие ее виды:

- изучение тем самостоятельной подготовки по учебно-тематическому плану;
- самоподготовка к практическим и другим видам занятий – расчетно-аналитическая работа по индивидуальному учебному заданию;
- самостоятельная работа слушателей при подготовке к итоговому тестированию.

Эти виды работ предполагают:

- самостоятельную работу слушателя в библиотеке;
- изучение материалов специализированных сайтов по темам дисциплины в сети Интернет;
- изучение электронных учебных материалов (электронных учебников, методических материалов, представленных на сайте УрСЭИ);

Задания для самостоятельной работы слушателей включают в себя:

- выполнение тестовых заданий, размещенных в программной оболочке Moodle – по темам, вынесенным на самостоятельное изучение;
- подготовка докладов по отдельным вопросам курса.

Указания и задания по самостоятельной работе выдаются на практических занятиях с учетом индивидуального уровня освоения материала слушателями.

Перечень вопросов для самостоятельной работы

1. Цели государства в области обеспечения информационной безопасности.
2. Основные нормативные акты РФ, связанные с правовой защитой информации.
3. Виды компьютерных преступлений.
4. Способы и механизмы совершения информационных компьютерных преступлений.
5. Основные параметры и черты информационной компьютерной преступности в России.
6. Компьютерный вирус. Основные виды компьютерных вирусов.
7. Методы защиты от компьютерных вирусов.
8. Типы антивирусных программ.
9. Защиты от несанкционированного доступа. Идентификация и аутентификация пользователя.
10. Основные угрозы компьютерной безопасности при работе в сети Интернет.
11. Виды защищаемой информации.
12. Государственная тайна как особый вид защищаемой информации.
13. Конфиденциальная информация.
14. Система защиты государственной тайны.
15. Правовой режим защиты государственной тайны.
16. Защита интеллектуальной собственности средствами патентного и авторского права.
17. Международное законодательство в области защиты информации.
18. Программно-аппаратные средства обеспечения информационной безопасности в информационных сетях.
19. Симметричные шифры.
20. Ассиметричные шифры.
21. Криптографические протоколы.
22. Криптографические хеш-функции.
23. Электронная подпись.
24. Организационное обеспечение информационной безопасности.
25. Служба безопасности организации.
26. Методы защиты информации от утечки в технических каналах.
27. Инженерная защита и охрана объектов.

Тема 1. Введение в информационную безопасность.

Вопросы для дискуссии

Что такое информационная безопасность?

2. Перечислите основные угрозы информационной безопасности. 3. Какие существуют модели информационной безопасности?
4. Какие методы защиты информации выделяют?
5. Что такое правовые методы защиты информации?
6. Что такое организационные методы защиты информации?
7. Что такое технические методы защиты информации?
8. Что такое программно-аппаратные методы защиты информации?
9. Что такое криптографические методы защиты информации?
10. Что такое физические методы защиты информации?
11. Какие главные государственные органы в области обеспечения информационной безопасности?
12. Перечислите виды защищаемой информации.

Тема 2. Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности.

Практические задания

На основе предложенного описания предприятия и изученной нормативно-распорядительной документации в области обеспечения информационной безопасности, группе студентов по 2-3 человека необходимо разработать обобщенную политику организации системы защиты персональных данных предприятия.

Тема 3. Правовое обеспечение информационной безопасности.

Вопросы для дискуссии

1. Право. Источники права. 2. Какие основные законы в области защиты информации в РФ?
3. Перечислите основные цели и задачи РФ в области обеспечения информационной безопасности
4. Стратегия национальной безопасности. Доктрина информационной безопасности.
5. Что такое конфиденциальная информация?
6. Что такое персональные данные?
7. В каких случаях возможно использовать персональные данные без согласия обладателя?
8. Охарактеризуйте биометрические данные как персональные данные. 9. Что такое профессиональная тайна?
10. Что такое служебная тайна?
11. Что такое коммерческая тайна?
12. Что такое режим коммерческой тайны?
13. Что такое государственная тайна?
14. Опишите правовой режим государственной тайны. 15. ФЗ-149. 16. ФЗ-152. 17. ФЗ-98. 18. ФЗ-390. 19. ФЗ-395-1. 20. ФЗ-126. 21. ФЗ-374 и ФЗ-375. 22. Постановление правительства №1119.

Тема 4. Использование криптографических средств защиты информации.

Практические задания

Студентам необходимо выполнить следующее рабочее задание использованием криптографического программного GnuPG под управлением ОС Linux Mint/Windows 7:

1. Сгенерируйте пару ключей (публичный, приватный) по типу «DSA and ElGamal» под именем user1.
2. Проверьте корректность характеристик ключей.
3. Зашифруйте обычный текстовый файл на открытом ключе пользователя user1. Затем расшифруйте его.
4. Подпишите ранее созданный текстовый файл и просмотрите файл с цифровой подписью.
5. Измените содержимое текстового файла и проверьте подлинность цифровой подписи.
6. Создайте архив (tar –cvf) и создайте для него цифровую подпись.
7. Проверьте подлинность цифровой подписи архива.
8. Создайте в каталоге /mnt подкаталог со своей фамилией.
9. Экспортируйте в созданный каталог свой открытый ключ.
10. Сгенерируйте также свои ключи, но под именем user2.
11. Из каталога /mnt/ФИО_студента импортируйте открытый ключ user1.
12. Убедитесь, что ключ добавился к вашему набору открытых ключей.
13. Зашифруйте file1 для пользователя user1 и сохраните его в директории /mnt/ФИО_студента.
14. Зашифруйте и подпишите file2 для пользователя user1.
15. Попробуйте расшифровать file1.asc и file2.asc при помощи ключа user2.
16. Перейдите в сеанс user1 и расшифруйте file1 и file2.
17. Подготовить отчет о проделанной работе.

Тема 5. Организационное обеспечение информационной безопасности.

Вопросы для дискуссии

1. Какие основные международные стандарты в области информационной безопасности?
2. "Оранжевая книга" 3. ISO/IEC 15408. 4. Как связаны международные стандарты и стандарты РФ?
5. ГОСТ Р ИСО/МЭК 27002-2012. 6. ГОСТ Р ИСО/МЭК 27005-2010. 7. СТО БР ИББС-1.1-2007. «Аудит информационной безопасности». 8. РС БР ИББС-2.2-2009. «Методика оценки рисков нарушения информационной безопасности». 9. Приказ ФСБ №378. 10. Приказ ФСТЭК №21. 11. Приказ ФСТЭК №17. 12. Приказ ФСТЭК №31. 13. Приказ ФСТЭК №28. 14. Приказ ФСТЭК №638. 15. Приказ ФСТЭК №9. 16. Приказ ФСТЭК №119. 17. Приказ Гостехкомиссии №114. 18. Руководящие документы Гостехкомиссии. 19. Меры защиты информации в государственных информационных системах. (Методический документ ФСТЭК). 20. Что такое политика безопасности?
21. Служба безопасности предприятия. Структура. Функции. 22. Типовая инструкция сотрудника по обеспечению информационной безопасности. 23. Экономическая разведка. Промышленный шпионаж

Тема 6. Реализация работы инфраструктуры открытых ключей.

Практические задания

Студентам необходимо выполнить следующее рабочее задание использованием криптографической библиотеки OpenSSL под управлением ОС Linux Mint/Windows 7:

1. Установить OpenSSL
2. Настроить СКЗИ (исправить файл openssl.cnf)
3. Подготовить окружение
4. Сформировать закрытый ключ УЦ
5. Сформировать запрос на сертификат УЦ. При этом использовать следующую информацию: Country: RU State: на ваш выбор Locality: на ваш выбор Organization: на ваш выбор Organization Unit: на ваш выбор Common Name: < Ваша Фамилия и Имя> CA 1 Email: < ваш e-mail>
6. Выпустить самоподписанный сертификат УЦ
7. Сформировать ключи, запросы на сертификат и сертификаты не менее чем двум пользователям. В качестве имен пользователей рекомендуется использовать вымышленные, но осмысленные имена.
8. Отозвать один из сертификатов пользователей.
9. Сформировать список отозванных сертификатов.
10. Создать документ формата .txt и заполнить его данными. Получить открытый ключ для секретного ключа пользователя, созданного в ходе выполнения предыдущей работы.
11. Сформировать подпись созданного на шаге 10 документа.
12. Проверить подпись документа.
13. Подготовить отчет о проделанной работе.

Тема 7. Технические средства и методы защиты информации.

Вопросы для дискуссии

1. Что такое инженерная защита объектов?
2. Каким способом описывается инженерная защита. Описать модель.
3. Какие средства применяются для защиты 1-го периметра?
4. Какие средства применяются для защиты 2-го периметра?
5. Какие средства применяются для защиты 3-го периметра?
6. Пожарные сигнализации. 7. Охранные сигнализации
8. Биометрия. Биометрические характеристики. 9. Что такое технические каналы утечки информации?
10. Перечислите основные виды технических каналов утечки информации?
11. Что такое спецпроверка?
12. Что такое специсследование?
13. Что такое спецобследование?
14. Перечислите методы защиты информации от утечки по зрительному каналу.
15. Перечислите методы защиты информации от утечки по электромагнитному каналу.
16. Перечислите методы защиты информации от утечки по электрическому каналу.
17. Перечислите методы защиты информации от утечки по индукционному каналу
18. Перечислите методы защиты информации от утечки по параметрическому каналу.
19. Перечислите методы защиты информации от утечки по воздушному каналу.
20. Перечислите методы защиты информации от утечки по вибрационному каналу.
21. Перечислите методы защиты информации от утечки по акустоэлектрическому каналу.
22. Перечислите методы защиты информации от утечки по оптикоэлектронному каналу.
23. Перечислите средства и методы защиты информации от утечки информации в телефонных линиях.

Тема 8. Средства стеганографии для защиты информации.

Практические задания

Студентам необходимо выполнить следующее рабочее задание использованием стеганографических программных средств под управлением ОС Linux Mint:

1. Создать документ формата .txt и наполнить его данными.
2. Установить TrueCrypt.
3. Создать контейнер. Имя – Фамилия студента. Алгоритм шифрования – AES. Хеш-функция – SHA-512. Размер - необходимый. Пароль – по усмотрению.
4. Зашифровать созданный документ с помощью TrueCrypt.
5. Установить VeraCrypt.
6. Создать контейнер. Имя – Фамилия студента. Алгоритм шифрования – AES. Хеш-функция – Streebog. Размер - необходимый. Пароль – ключевой файл.
7. Зашифровать созданный документ с помощью VeraCrypt.
8. Зашифровать созданный документ с помощью BitLocker.
9. Установить ViPNet SafeDisk.
10. Создать контейнер. Имя – Фамилия студента. Алгоритм шифрования – ГОСТ. Размер – необходимый. Пароль – по усмотрению.
11. Установить Image Spyer.
12. Сконфигурировать Image Spyer.
13. Замаскировать некоторое сообщение с помощью Image Spyer.
14. Извлечь сообщения из стеганоcontainers.
15. Сократить информацию с помощью OpenPuff в аудиофайле.
16. Добавить в этот же аудиофайл цифровой водяной знак.
17. Проверить правильность выполнения задания.
18. Подготовить отчет о проделанной работе. К отчету приложить все зашифрованные стеганофайлы, а также все пароли от зашифрованных и замаскированных сообщений.

Тема 9. Программно-аппаратные средства и методы обеспечения информационной безопасности.

Вопросы для дискуссии

1. Что такое программно-аппаратные средства защиты информации?
2. Какие механизмы реализуют программно-аппаратные средства защиты информации?
3. Какие компьютерные угрозы безопасности существуют?
4. Что такое сетевая разведка? Какие методы защиты против нее существуют?
5. Что такое инъекция? Какие виды инъекций существуют? Какие методы защиты против них существуют?
6. Что такое отказ в обслуживании? Какие методы защиты против него существуют?
7. Основные виды программных уязвимостей. 8. Бэкдоры. 9. Что такое переполнение буфера? Методы защиты. 10. Что такое дефекты форматных строк? Методы защиты. 11. Что такое целочисленные переполнения? Методы защиты. 12. Ошибки обработки исключений. Методы защиты. 13. Внедрение команд. Методы защиты. 14. Некорректные обработки ошибок. Методы защиты. 15. Гонки. Методы защиты. 16. Выполнение кода с завышенными привилегиями. 17. Атака "Человек по середине". 18. Что такое IP-спуффинг? Какие методы защиты против него существуют?
19. ARP. 20. DHCP. 21. NAT. 22. PAT. 23. IPv4. IPv6. 24. Что такое ARP-спуффинг? Какие методы защиты против него существуют?
25. Что такое DNS Cache Poisoning? Какие методы защиты против него существуют?
26. Что такое NetBIOS/NBNS spoofing? Какие методы защиты против него существуют?
27. VPN. 28. Социальная инженерия. 29. Фрод. Методы борьбы с фродом. 30. Что такое фишинг? Какие методы защиты против него существуют?
31. Кардинг. Методы защиты от кардинга. 32. Darkweb. 33. DMZ. 34. Анонимайзеры. 35. Прокси-серверы. 36. Резервное копирование. 37. Honey pot. 38. DLP-системы. SIEM-системы. 39. Сканеры безопасности. 40. Системы обнаружения вторжений. 41. Системы предотвращения вторжений. 42. Вредоносные программы. Компьютерные вирусы. Виды вирусов. 43. Эксплоиты. 44. Механизм работы вируса. 45. Антивирусы. Виды антивирусов. 46. Механизмы работы антивируса. 47. Межсетевой экран.

Тема 10. Настройка безопасного сетевого соединения.

Практические задания

Имеются две локальные сети. В каждой из них есть сервер с установленным Kerio Winroute Firewall, с предустановленным VPN сервером. Студентам необходимо выполнить следующее рабочее задание под управлением ОС Linux Mint:¶1. Объедините две локальные сети друг с другом, чтобы пользователи имели доступ к компьютерам и серверам из разрозненных сетей. Для этих задач нужно создать между двумя серверами, подключенными к Интернет, VPN Туннель.¶2. На одну из виртуальных машин установите web-сервер <sudo apt-get install apache2>.¶3. На другую установите – Nmap <sudo apt-get install nmap>.¶4. Определите IP адрес виртуальной машины, где установлен web-сервер apache.¶5. Произведите сканирование web-сервера всеми описанными методами (Изучение средств сканирования Nmap).¶6. Установите Honeyd.¶7. Ознакомьтесь с информацией по настройке Honeyd и стандартным содержимым файла /etc/honeypot/honeyd.conf.¶8. Настройте Honeyd изменив содержание файла /etc/honeypot/honeyd.conf .¶9. Запустите <farpd -d>.¶10. Запустите honeyd. <honeyd -d -f /etc/honeypot/honeyd.conf>¶11. Произведите сканирование сети с honeypot.¶12. Измените настройки Honeyd. Усложните конфигурационный файл. Добавьте несколько ловушек, измените информацию об ОС, информацию о роутере, об открытых портах и.т.д.¶13. Запустите honeyd. <honeyd -d -f /etc/honeypot/honeyd.conf>¶14. Произведите сканирование.¶15. Подготовить отчет о проделанной работе.¶

Тема 11. Криптографические методы защиты информации.

Вопросы для дискуссии

1. Что такое шифр? Какие виды шифров существуют?
2. Что такое симметричный шифр? Какие симметричные шифры используются сейчас?
3. Что такое асимметричный шифр? Какие асимметричные шифры используются сейчас?
4. Принцип построения симметричных шифров. 5. Принцип построения асимметричных шифров. 6. Стандартные шифры. 7. Поточные шифры. 8. Что такое хеш-функция? Какие виды хеш-функций вы знаете?
9. Дерево Меркла. 10. Что такое цифровая подпись?
11. Цифровая подпись RSA. 12. Цифровая подпись Эль-Гамала. 13. Что такое инфраструктура открытых ключей?
14. Жизненный цикл ключа. 15. Аутентификация, идентификация, верификация, авторизация. 16. Простейшие протоколы идентификации. 17. Основной протокол Kerberos. 18. IPSec. 19. Blockchain.
20. Что такое стеганография? Понятие стеганоконтейнера. 21. Какие виды стеганоконтейнеров существуют?
22. Методы создания стеганоконтейнеров на основе текстовой информации. 23. Методы создания стеганоконтейнеров на основе видеоинформации и стоп/кадров. 24. Методы создания стеганоконтейнеров на основе аудиоинформации. 25. Цифровые водяные знаки.

Тема 12. Антивирусные средства защиты информации.

Практические задания

Студентам необходимо выполнить следующее рабочее задание с использованием программного средства Kaspersky Endpoint Security и Kaspersky Security Center под управлением ОС Windows 7: ¶1. Осуществите локальную установку Kaspersky Endpoint Security.¶2. Внедрите модуль управления Kaspersky Security Center.¶3. Создайте структуру управляемых компьютеров.¶4. Настройте модуль «Защиты от файловых угроз».¶5. Настройте задачи поиска вирусов.¶6. Настройте исключения для выбранной папки.¶7. Настройте модуль «Защиты от почтовых угроз».¶8. Настройте защиту от программ вымогателей.¶9. Настройте защиту от сетевых угроз.¶10. Настройте сетевой экран для мобильной политики.¶11. Настройте исключения из самозащиты.¶12. Настройте защиту паролем для KES.¶13. Настройте Контроль программ.¶14. Заблокируйте запуск неизвестных файлов в сети.¶15. Запретите доступ к съемным носителям информации.¶16. Настройте права к съемным носителям информации.¶17. Настройте контроль доступа к веб-ресурсам.¶18. Настройте дэшборд.¶19. Соберите журналы трассировки.¶20. Организуйте резервное копирование и восстановление Kaspersky Security Center.¶21. Подготовить отчет о проделанной работе.¶

7. ОСНОВНАЯ И ДОПОЛНИТЕЛЬНАЯ УЧЕБНАЯ ЛИТЕРАТУРА, НЕОБХОДИМАЯ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

Основная литература

1. Щербак, А. В. Информационная безопасность : учебник для вузов / А. В. Щербак. — 2-е изд. — Москва : Издательство Юрайт, 2026. — 252 с. — (Высшее образование). — ISBN 978-5-9916-4299-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/589902>.
2. Суворова, Г. М. Информационная безопасность : учебник для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 277 с. — (Высшее образование). — ISBN 978-5-534-16450-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/588515>.
3. Зенков, А. В. Информационная безопасность и защита информации : учебник для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/588741>.

4. Чернова, Е. В. Информационная безопасность человека : учебник для вузов / Е. В. Чернова. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 327 с. — (Высшее образование). — ISBN 978-5-534-16772-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/587699>.

Дополнительная литература

5. Целых, А. Н. Выявление инцидентов информационной безопасности и мошеннических транзакций методами машинного обучения : учебное пособие : [16+] / А. Н. Целых, Э. М. Котов ; Южный федеральный университет, Инженерно-технологическая академия. — Ростов-на-Дону : Южный федеральный университет, 2023. — 118 с. : ил., табл. — Режим доступа: по подписке. — URL: <https://biblioclub.ru/index.php?page=book&id=713464>. — Библиогр. в кн. — ISBN 978-5-9275-4515-5. — Текст : электронный.

6. Нормативное сопровождение информационной безопасности : учебное пособие : [16+] / С. И. Фокина, А. В. Выволокина, А. Ю. Гарькушев, А. В. Липис. — Москва ; Вологда : Инфра-Инженерия, 2025. — 136 с. : ил., табл. — Режим доступа: по подписке. — URL: <https://biblioclub.ru/index.php?page=book&id=725664>. — Библиогр. в кн. — ISBN 978-5-9729-2530-8. — Текст : электронный.

7. Организационное и правовое обеспечение информационной безопасности : учебник для вузов / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией Т. А. Поляковой, А. А. Стрельцова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 357 с. — (Высшее образование). — ISBN 978-5-534-19108-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/583236>.

8. ПЕРЕЧЕНЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ И ИНТЕРНЕТ - РЕСУРСОВ, НЕОБХОДИМЫХ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

Программное обеспечение

№	Наименование	Описание
1	Packet Tracer	Packet Tracer — симулятор сети передачи данных, выпускаемый фирмой Cisco Systems.
2	MS Office 2007 - 2019	Офисный пакет приложений, созданных корпорацией Microsoft для операционных систем Windows, Windows Phone, Android, macOS, iOS. В состав пакета входит ПО для работы с различными типами документов: текстами, электронными таблицами и др.
3	Microsoft Windows Server 2003, 2008, 2012	Линейка серверных операционных систем от компании Microsoft.
4	Linux Ubuntu, Linux Debian, Linux Mint	Семейство Unix-подобных операционных систем на базе ядра Linux, включающих тот или иной набор утилит и программ проекта GNU

510	MS Windows XP, Windows 8, Windows 10	Операционная система для персональных компьютеров и рабочих станций, разработанная корпорацией Microsoft в рамках семейства Windows.
-----	--------------------------------------	--

Интернет-ресурсы, информационные и справочные системы

№	Наименование	Описание
1	ИТ-портал «Сервер Информационных Технологий»	http://citforum.ru/
2	Виртуальная академия Microsoft	https://mva.microsoft.com/
3	Хранилище документации Майкрософт для пользователей, разработчиков и ИТ специалистов.	https://docs.microsoft.com/ru-ru/
4	Курс по компьютерным сетям начального уровня.	https://www.asozykin.ru/courses/networks_online

9. ТРЕБОВАНИЯ К МАТЕРИАЛЬНО-ТЕХНИЧЕСКОМУ И УЧЕБНО-МЕТОДИЧЕСКОМУ ОБЕСПЕЧЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Помещения, в которых проводятся занятия, представляют собой учебные аудитории для проведения учебных занятий. Данные аудитории оснащенные оборудованием и техническими средствами обучения.

Компьютеры, информационно-телекоммуникационные сети, аппаратно-программные и аудиовизуальные средства, находящиеся в учебных аудиториях:

- персональный компьютер или ноутбук (для преподавателя) с выходом в сеть интернет;
- проектор;
- акустическая система
- экран для проектора;
- доска маркерная (ученическая доска);

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой и имеют возможность подключения к сети интернет и обеспечивают доступ к электронной информационно-образовательной среде академии.

10. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В процессе освоения дисциплины используются следующие образовательные технологии:

- Технология коммуникативного обучения – направлена на формирование коммуникативной компетентности студентов, которая является базовой, необходимой для адаптации к современным условиям межкультурной коммуникации.
- Технология разноуровневого (дифференцированного) обучения – предполагает осуществление познавательной деятельности студентов с учётом их индивидуальных способностей, возможностей и интересов, поощряя их реализовывать свой творческий потенциал.
- Технология индивидуализации обучения – помогает реализовывать личностно-ориентированный подход, учитывая индивидуальные особенности и потребности учащихся.
- Технология модульного обучения – предусматривает деление содержания дисциплины на достаточно автономные разделы (модули), интегрированные в общий курс.
- Игровая технология – позволяет развивать навыки рассмотрения ряда возможных способов решения проблем, активизируя мышление студентов и раскрывая личностный потенциал каждого обучаемого.
- Информационно-коммуникационные технологии (ИКТ) расширяют рамки образовательного процесса, повышая его практическую направленность, способствуют интенсификации самостоятельной работы обучаемых и повышению познавательной активности
- Технология тестирования – используется для контроля уровня усвоения лексических, грамматических знаний в рамках раздела на определенном этапе обучения.
- Проектная технология – ориентирована на моделирование социального взаимодействия обучаемых с целью решения задачи, которая определяется в рамках профессиональной подготовки студентов, выделяя ту или иную предметную область. Использование проектной технологии способствует реализации междисциплинарного характера компетенций, формирующихся в процессе обучения иностранному языку.
- Технология развития критического мышления – способствует формированию разносторонней личности, способной критически относиться к информации, умению отбирать информацию для решения поставленной задачи.

Для повышения мотивации и активности студентов на занятиях используются групповые, проектные задания, учебные конференции, дискуссии, ролевые игры и т.д., а также в систему аудиторной и самостоятельной работы внедряются ИКТ и современные цифровые ресурсы.

11. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Код ком п.	Идентиф.	Тип задания	Уровень	Время (мин)	Задание	Ключ
УК-2	Знать	Задание закрытого типа на установление соответствия	Базовый	3	Установите соответствие между видами защищаемой информации (А–Г) и нормативными актами, их регулирующими (1–4). Виды: А) Государственная тайна; Б) Персональные	А-2, Б-1, В-3, Г-4

					данные; В) Коммерческая тайна; Г) Профессиональная тайна. Акты: 1) ФЗ от 27.07.2006 № 152-ФЗ; 2) Закон РФ от 21.07.1993 № 5485-1; 3) ФЗ от 29.07.2004 № 98-ФЗ; 4) Основы законодательства РФ о нотариате.	
УК-2	Знать	Задание комбинированного типа с выбором одного верного ответа и обоснованием	Базовый	2	К правовым методам, обеспечивающим информационную безопасность, относятся: 1) Разработка аппаратных средств обеспечения правовых данных; 2) Разработка и установка во всех компьютерных правовых сетях журналов учёта действий; 3) Разработка и конкретизация правовых нормативных актов обеспечения безопасности; 4) Обучение персонала.	Ответ: 3. Обоснование: Правовые методы — это нормы права, регулирующие отношения в информационной сфере (ФЗ от 27.07.2006 № 149-ФЗ).
УК-2	Уметь	Задание закрытого типа на установление соответствия	Базовый	3	Установите соответствие между понятиями (А–В) и их характеристиками (1–3). Понятия: А) Компьютерные сети; Б) Базы данных; В) Информационные системы. Характеристики: 1)	А-2, Б-1, В-3

					Таблицы и структуры данных, SQL, индексы и оптимизация запросов; 2) Протоколы передачи данных, маршрутизаторы и коммутаторы, IP-адреса; 3) CRM, ERP, BI.	
УК-2	Уметь	Задание комбинированного типа с выбором одного верного ответа и обоснованием	Повышенный	5	Организация хочет защитить коммерческую тайну. Какие действия необходимо предпринять в первую очередь? Варианты: 1) Ввести режим коммерческой тайны; 2) Опубликовать сведения в открытом доступе; 3) Передать данные в государственные органы; 4) Зашифровать все данные без анализа.	Ответ: 1. Обоснование: Согласно ст. 10 ФЗ от 29.07.2004 № 98-ФЗ «О коммерческой тайне», для защиты информации необходимо ввести режим коммерческой тайны.
УК-2	Практический опыт	Задание открытого типа	Высокий	8	Опишите порядок действий при выявлении утечки персональных данных в организации.	1) Немедленно уведомить руководство и ответственного за обработку ПДн; 2) Провести внутреннее расследование; 3) Уведомить Роскомнадзор (в течение 24 часов); 4) Принять меры по устранению последствий; 5) Обновить политику безопасности.

УК-10	Знать	Задание комбинированного типа с выбором нескольких верных ответов и развёрнутым обоснованием	Базовый	3	Выберите правильные ответы. Виды информационной безопасности включают: а) персональная; б) серверная; в) корпоративная; г) государственная.	Ответы: а, в, г. Обоснование: Виды информационной безопасности выделяются по уровню субъекта: личность (персональная), организация (корпоративная), государство (государственная). Серверная — не является видом ИБ.
УК-10	Знать	Задание закрытого типа на установление последовательности	Базовый	3	Упорядочите этапы в процессе обеспечения информационной безопасности: 1) Идентификация и анализ уязвимостей системы; 2) Разработка и внедрение политики безопасности; 3) Резервное копирование и защита данных; 4) Мониторинг и обнаружение инцидентов безопасности.	2, 1, 3, 4
УК-10	Уметь	Задание комбинированного типа с выбором одного верного ответа и обоснованием	Повышенный	3	Что такое коррупционное поведение? Варианты: 1) Злоупотребление служебным положением; 2) Дача взятки; 3) Получение взятки; 4) Все перечисленное.	Ответ: 4. Обоснование: Согласно ст. 1 ФЗ от 25.12.2008 № 273-ФЗ «О противодействии коррупции», коррупция включает злоупотребление положением, дачу и получение взятки.

УК-10	Уметь	Задание комбинированного типа с выбором нескольких верных ответов и развёрнутым обоснованием	Повышенный	5	Какие признаки указывают на коррупционное поведение? Выберите два: 1) Конфликт интересов; 2) Личная заинтересованность; 3) Благотворительность; 4) Подарки стоимостью до 3 тыс. руб.	Ответы: 1, 2. Обоснование: Конфликт интересов и личная заинтересованность — признаки коррупции (ст. 10, 11 ФЗ № 273-ФЗ). Благотворительность и подарки до 3 тыс. руб. не являются коррупцией.
УК-10	Практический опыт	Задание открытого типа	Высокий	8	Предложите меры по нейтрализации коррупционного поведения в организации.	1) Внедрение кодекса этики; 2) Обучение сотрудников; 3) Создание комиссии по конфликту интересов; 4) Анонимная горячая линия; 5) Регулярные проверки.
ОПК-3	Знать	Задание открытого типа	Повышенный	4	Дополните определение. _____ — это комплекс руководств и требований обеспечения необходимого уровня безопасности.	Политика безопасности в системе (сети).
ОПК-3	Знать	Задание комбинированного типа с выбором одного верного ответа и обоснованием	Базовый	2	Утечкой информации в системе называется ситуация, характеризующаяся: 1) Потерей данных в системе; 2) Изменением формы информации; 3) Несанкционированным доступом к информации; 4) Изменением	Ответ: 3. Обоснование: Утечка — это неправомерный доступ к охраняемой информации (ФЗ № 149-ФЗ).

					содержания информации.	
ОПК -3	Уметь	Задание комбинированного типа с выбором одного верного ответа и обоснованием	Повышенный	5	Что следует сделать, если вы получили спам по e-mail с приложенным файлом? Варианты: 1) Открыть вложение и проверить; 2) Удалить письмо, не открывая вложение; 3) Переслать коллегам; 4) Ответить отправителю.	Ответ: 2. Обоснование: Вложение может содержать вредоносное ПО. Безопаснее удалить письмо, не открывая его.
ОПК -3	Уметь	Задание закрытого типа на установление соответствия	Повышенный	4	Установите соответствие между типами угроз (А–Г) и их примерами (1–4). Угрозы: А) Вирусы; Б) Фишинг; В) Социальная инженерия; Г) Сетевые атаки. Примеры: 1) Звонок от «службы безопасности»; 2) Письмо с просьбой перейти по ссылке; 3) DDoS-атака; 4) Троянская программа.	А-4, Б-2, В-1, Г-3
ОПК -3	Практический опыт	Задание комбинированного типа с выбором нескольких верных ответов и развёрнутым обоснованием	Повышенный	5	Какие методы защиты от вредоносных программ существуют? Выберите три: 1) Антивирусное ПО; 2) Фаервол; 3) Регулярные	Ответы: 1, 2, 3. Обоснование: Антивирус, фаервол и обновления — стандартные методы. Отключение от сети — крайняя

					обновления ПО; 4) Отключение от сети.	мера, не является методом защиты.
ОПК -3	Практическ ий опыт	Задание открытого типа	Высокий	8	Поясните, что такое ЭЦП и какие задачи она решает.	ЭЦП — метод аутентификации и обеспечения целостности данных. Решает задачи: подтверждение авторства, контроль неизменности документа, юридическая значимость.