МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ,
МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ КЫРГЫЗСКОЙ РЕСПУБЛИКИ

ГОУ ВПО Кыргызско-Российский Славянский университет

Информационная безопасность

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Информатики**

Учебный план Направление 41.03.05 Международные отношения

Квалификация **бакалавр**

Форма обучения **очная**

Общая трудоемкость **2 ЗЕТ**

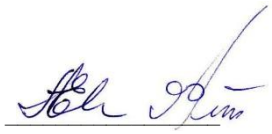
Часов по учебному плану 72
в том числе:
аудиторные занятия 36
самостоятельная работа 36

Виды контроля в семестрах:
зачеты 3

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**3 (2.1)**		Итого	
Недель	18			
Вид занятий	УП	РПД	УП	РПД
Лекции	18	18	18	18
Практические	18	18	18	18
В том числе инт.	8	8	8	8
Итого ауд.	36	36	36	36
Контактная	36	36	36	36
Сам. работа	36	38	36	38
Итого	72	74	72	74

Программу составил(и):

к.т.н, доцент, зав.кафедрой , Евтушенко А.И.;ст.преподаватель , Фейгин Я.Д. 

Рецензент(ы):
д.ф-м.н, профессор , Усманов С.Ф. 

Рабочая программа дисциплины

Информационная безопасность

составлена на основании учебного плана:
Направление 41.03.05 Международные отношения
утвержденного учёным советом вуза от 29.05.2015 протокол № 11.

Рабочая программа одобрена на заседании кафедры

Информатики

Протокол от 10 __09_____ 2015г. № 2
Срок действия программы: 2015-2020 уч.г.
Зав. кафедрой Евтушенко А.И. 

Визирование РПД для исполнения в очередном учебном году

Председатель УМС
13 09 2016 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2016-2017 учебном году на заседании кафедры
Информатики

Протокол от 11 09 2016 г. № 2
Зав. кафедрой Евтушенко А.И.

Визирование РПД для исполнения в очередном учебном году

Председатель УМС
12 09 2017 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2017-2018 учебном году на заседании кафедры
Информатики

Протокол от 30.10 2017 г. № 2
Зав. кафедрой Евтушенко А.И.

Визирование РПД для исполнения в очередном учебном году

Председатель УМС
10 09 2018 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2018-2019 учебном году на заседании кафедры
Информатики

Протокол от 22 июня 2018 г. № 8
Зав. кафедрой Евтушенко А.И.

Визирование РПД для исполнения в очередном учебном году

Председатель УМС
__ _____ 2019 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2019-2020 учебном году на заседании кафедры
Информатики

Протокол от __ _____ 2019 г. № __
Зав. кафедрой Евтушенко А.И.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	Основной целью дисциплины является ознакомление студентов с тенденцией развития информационной безопасности, с моделями возможных угроз, терминологией и основными понятиями теории безопасности информации, а так же с нормативными документами России и Кыргызстана по данному вопросу.
1.2	Изучение дисциплины «Информационная безопасность» направлено на решение следующих задач:
1.3	¯ получения студентами знаний по существующим угрозам безопасности информации, подбору и применению современных методов и способов защиты информации;
1.4	¯ формирование навыковбезопасной работы в различных сетевых структурах, в т.ч. и социальных сетях

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП	
Цикл (раздел) ООП:	Б1.Б.04
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Информатика
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Информационно-аналитическая работа

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
ОК-5: владением основными методами, способами и средствами получения, хранения, переработки информации, навыками работы с компьютером как средством управления информацией; способностью работать с информацией в глобальных компьютерных сетях	
Знать:	
Уровень 1	основы информационно-коммуникационных технологий, приемы безопасной работы в локальных и глобальных сетях
Уровень 2	программные и аппаратные средства получения, хранения и переработки информации с учетом всех требований информационной безопасности
Уровень 3	концепции современной информационной безопасности; методы и технологии (парольные, криптографические, стеганографические) защиты компьютерной информации
Уметь:	
Уровень 1	применять на практике информационно-коммуникационные технологии для безопасной работы в локальных и глобальных сетях
Уровень 2	использовать современные программные и аппаратные средства получения, хранения и переработки информации с учетом всех требований информационной безопасности
Уровень 3	использовать парольные, криптографические, стеганографические технологии защиты компьютерной информации при ее хранении и передаче
Владеть:	
Уровень 1	приемами безопасной работы в локальных и глобальных сетях
Уровень 2	навыками использования современных программных и аппаратные средств получения, хранения и переработки информации с учетом всех требований информационной безопасности
Уровень 3	навыками использования парольных, криптографических, стеганографических технологий защиты компьютерной информации при ее хранении и передаче

ОПК-8: способностью понимать сущность и значение информации в развитии современного информационного общества, сознавать опасности и угрозы, возникающие в этом процессе, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны	
Знать:	
Уровень 1	основные понятия и определения, используемые при изучении информационной безопасности; классификацию угроз информационной безопасности; как организовать информационную безопасность на предприятии
Уровень 2	криптографические и стеганографические методы защиты информации при передаче
Уровень 3	классификацию "компьютерных вирусов", какую угрозу они представляют для безопасности информации и правила защиты от "компьютерных вирусов"; методы социальной инженерии и способы и приемы безопасной работы в сети
Уметь:	
Уровень 1	подключить организацию к Internet с соблюдением требований информационной безопасности
Уровень 2	применять криптографические средства защиты от несанкционированного доступа при передаче данных через Интернет, квалифицированно использовать парольные средства защиты при хранении данных на компьютере
Уровень 3	правильно выбрать и использовать антивирусную программу

Владеть:	
Уровень 1	методами организации безопасной работы в локальнных АИС на предприятии
Уровень 2	парольными и криптографическими средствами защиты от несанкционированного доступа прихранении данных и при передаче через Интернет
Уровень 3	антивирусными средствами защиты компьютера

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	иметь представление:
3.1.2	о концепциях современной информационной безопасности;
3.1.3	о месте, роли и тенденциях развития методов и технологий защиты компьютерной информации;
3.1.4	об особенностях и проблемах защиты информации в будущей профессиональной деятельности;
3.1.5	знать:
3.1.6	фундаментальные понятия информационной безопасности;
3.1.7	основные принципы и правила хранения, передачи и защиты компьютерной правовой информации;
3.1.8	состав, функции и конкретные возможности аппаратно-программного обеспечения в процессе решения задач профессионально-служебной деятельности;
3.1.9	основные нормативные документы, законы и указы, регламентирующие организацию защиты информации.
3.2	**Уметь:**
3.2.1	•использовать современные аппаратно-программные средства в области защиты информации
3.2.2	•грамотно управлять системой защиты информации при работе на персональном компьютере
3.2.3	•выявлять и классифицировать источники внешних и внутренних угроз
3.2.4	•защищать информационные ресурсы от вредоносного программного обеспечения.
3.3	**Владеть:**
3.3.1	•использования основных защитных механизмов, мер и средств обеспечения информационной безопасности
3.3.2	•комплексного подхода к построению системы защиты информации
3.3.3	•использования криптографических методов защиты информации
3.3.4	.использования парольных и биометрических методов защиты информации

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература	Инте ракт.	Примечание
	Раздел 1. Введение в информационную безопасность. Криптография						
1.1	Введение в информационную безопасность. Основные понятия. /Лек/	3	2	ОК-5	Л1.1 Л2.1 Э1	0	
1.2	1. Классификация угроз информационной безопасности 2. Каналы утечки информации /Пр/	3	2	ОК-5	Л1.1 Э1	0	
1.3	Способы раскрытия преступлений в сфере компьютерной информации. /Ср/	3	4	ОК-5	Л1.1 Л2.1 Э1	0	
1.4	Принципы построения защищенной АИС /Лек/	3	2	ОК-5	Л1.2 Л2.2 Э1	2	Организационная форма - разбор конкретных ситуаций (АИС КРСУ)
1.5	1. Меры противодействия угрозам безопасности. 2. Политика безопасности. /Пр/	3	2	ОПК-8	Л1.3 Л2.2 Л3.1 Э1	0	
1.6	Хакеры и хакерское сообщество. /Ср/	3	4	ОПК-8	Л2.2 Л2.1 Л3.1 Э1	0	

1.7	Криптографические методы защиты информации. /Лек/	3	2	ОПК-8	Л1.2 Л3.2 Э2	2	Организационная форма - разбор конкретных ситуаций (безопасность переписки студента в Интернете)
1.8	1.Основные понятия криптографии, область применения. 2.Классификация методов криптозащиты. 3. Методы подстановки /Пр/	3	2	ОПК-8	Л1.4 Л2.3 Л3.2 Э2	0	
1.9	Пропорциональные шифры. /Ср/	3	2	ОПК-8	Л1.5 Л2.4 Э2	0	
1.10	Симметричные алгоритмы шифрования /Лек/	3	4	ОПК-8	Л1.5 Л2.4 Л3.1 Э2	0	
1.11	Симметричные алгоритмы шифрования /Пр/	3	4	ОПК-8	Л1.5 Л2.3 Э2	4	Организационная форма - ролевая игра (шифровальщик - дешифрофщик)
1.12	Ассиметричная криптография /Ср/	3	6	ОПК-8	Л1.7 Э2	0	
1.13	Альтернативы алгоритму RSA /Ср/	3	4	ОПК-8	Л2.4 Л3.1 Э2	0	
1.14	Стеганография /Лек/	3	2	ОПК-8	Л2.4 Э2	0	
1.15	Работа со стеганографическими программами /Пр/	3	2	ОПК-8	Л1.5 Э2	0	
1.16	Микроточки в стеганографии /Ср/	3	4	ОПК-8	Л1.5 Л3.1 Э2	0	
	Раздел 2. Антивирусная защита. Средства защиты сети. Социальный инжиниринг						
2.1	Компьютерные вирусы и борьба с ними. /Лек/	3	2	ОПК-8	Л1.5 Л1.7 Л3.2 Э3	0	
2.2	1.Классификация вирусов. 2.Файловые вирусы Макровирусы. Сетевые черви. 3.Технологии маскировки вирусов. 4.Борьба с вирусами /Пр/	3	2	ОПК-8	Л1.5 Л1.7 Л2.2 Л3.1 Э3	0	
2.3	История появления вирусов и антивирусных программ /Ср/	3	4	ОПК-8	Л1.8 Л3.2 Э3	0	
2.4	Средства защиты сети. /Лек/	3	2	ОПК-8	Л1.8 Э4	0	
2.5	1. Межсетевые экраны. Брендмауэр OutPost. 2. Виртуальные частные сети. 3. DOS и DDOS атаки. /Пр/	3	2	ОПК-8	Л1.8 Л2.2 Л3.1 Э4	0	
2.6	Социальный инженириг. /Лек/	3	2	ОПК-8 ОК-5	Л1.1 Л3.1 Э3 Э5	0	

2.7	1. Способы атаки на пароль. Обеспечение безопасности пароля. 2. Социальный инжиниринг 3. Сбор паролей, хранящихся в общедоступных местах. 4. Фишинг. /Пр/	3	2	ОПК-8 ОК-5	Л1.1 Э5	0	
2.8	Меры противодействия фишингу. /Ср/	3	4	ОПК-8 ОК-5	Л1.2 Э5	0	
2.9	Подготовка к круглому столу. Создание презентаций /Ср/	3	6	ОПК-8 ОК-5	Л1.2 Э1 Э2 Э3 Э4 Э5	0	
2.10	Опрсо для проверки уровней обученности Знать, Уметь, Владеть /Зачёт/	3	0	ОК-5 ОПК-8	Э1 Э2 Э3 Э4 Э5	0	

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

5.1. Контрольные вопросы и задания

Вопросы для проверки уровня обученности Знать

1. Понятия конфиденциальности, целостности, доступности информации.
2. Угрозы информационной безопасности, их классификация.
3. Каналы утечки информации
4. Неформальная модель нарушителя.
5. Информационная безопасность на уровне государства
6. Задачи системы информационной безопасности.
7. Меры противодействия угрозам безопасности.
8. Политика безопасности.
9. Основные принципы построения систем защиты АИС
10. Основные понятия криптографии, область применения.
11. Периодизация истории криптографии.
12. Классификация методов криптозащиты.
13. Симметричные алгоритмы.
14. Методы подстановки
15. Методы перестановки,
16. Блочные шифры
17. Поточные шифры.
18. Криптографические атаки.
19. Проблемы симметричного шифрования.
20. Принципы шифрования с открытым ключом.
21. Схема ассиметричного шифрования.
22. Алгоритм RSA.
23. Электронно-цифровая подпись. Удостоверяющие центры.
24. Криптографические протоколы
25. Основные понятия стеганографии, область применения.
26. Классификация стеганографических методов.
27. Компьютерная стеганография.
28. Цифровые водяные знаки.
29. Классификация вирусов.
30. Файловые вирусы Макровирусы. Сетевые черви.
31. Загрузочные вирусы. Троянские кони.
32. Технологии маскировки вирусов. Тенденции современных компьютерных вирусов.
33. Борьба с вирусами
34. Межсетевые экраны. Брендмауэр OutPost.
35. Виртуальные частные сети.
36. Системы обнаружения вторжений. DOS и DDOS атаки.
37. Парольная защита Способы атаки на пароль.
38. Обеспечение безопасности пароля.
39. Сбор паролей, хранящихся в общедоступных местах.
40. Фишинг.

Примерный перечень заданий для проверки уровней обученности Уметь и Владеть (в компьютерных дисциплинах они совпадают)

1. Определить, нарушением какого свойства информации является данная ситуация.
2. Определить типы угроз информационной безопасности по данной ситуации.
3. Определить возможные каналы утечки информации в заданной преподавателем ситуации

4. Построить неформальную модель нарушителя информационной безопасности по заданной преподавателем ситуации
5. Определить приоритетные задачи информационной безопасности для заданной преподавателем АИС
6. Определить меры противодействия угрозам безопасности в заданной преподавателем ситуации
7. Определить приоритетные задачи политики безопасности в заданной преподавателем ситуации
8. Провести шифрование/расшифрование методом Цезаря
9. Провести шифрование/расшифрование указанным методом одноалфавитной подстановки
10. Провести шифрование/расшифрование методом пропорциональных шифров
11. Провести шифрование/расшифрование методом Вижинера
12. Провести шифрование/расшифрование методом простой перестановки
13. Провести шифрование/расшифрование методом табличной перестановки.
14. Провести шифрование/расшифрование блочными алгоритмами
15. Определить наличие вложений в стегоконтейнере
16. Поместить указанные преподавателем вложения в стегоконтейнер
17. Определить наличие цифровых водяных знаков в данных файлах
18. Поставить цифровые водяные знаки в указанные файлы
19. Провести антивирусную проверку указанного сектора компьютерного диска
20. Определить надежность парольной защиты в заданной преподавателем ситуации

5.2. Темы курсовых работ (проектов)

не предусмотрены

5.3. Фонд оценочных средств

ТЕСТ

Образцы тестовых заданий по темам информационной безопасности даны в приложении 1

ПРЕЗЕНТАЦИЯ

темы презентаций:

1. Нормативно-правовые аспекты информационной безопасности
2. Мотивы и цели компьютерных преступлений
3. Особенности личности преступника, совершающего компьютерные преступления
4. Статьи уголовного кодекса о компьютерных преступлениях
5. Уголовно-правовая характеристика преступлений в сфере компьютерной информации и их предупреждение
6. Способы раскрытия преступлений в сфере компьютерной информации.
7. Киберпреступность в современном мире
8. Криминологический анализ преступлений в сфере компьютерной информации
9. Внешние угрозы информационной безопасности
10. Человеческие факторы, обуславливающие информационные угрозы
11. Предупреждение компьютерных преступлений
12. Государственное регулирование информационной безопасности в разных странах
13. Охраняемая законом информация, виды тайн, охраняемых законом
14. Субъективная сторона компьютерных преступлений
15. Хакеры
16. Хакерские сообщества
17. Самые вредоносные и разрушительные вирусы за последние десятилетия.
18. Объективная сторона компьютерных преступлений
19. Причины и условия, способствующие совершению компьютерных преступлений
20. Меры предупреждения преступлений в сфере компьютерной информации
21. История вредоносных программ (не только вирусов!).
22. Исторические аспекты компьютерных преступлений
23. Причины разглашения конфиденциальной информации
24. Разглашение и утечка информации
25. Электронно-цифровая подпись, ее виды, особенности применения.
26. Оценка эффективности инвестиций в информационную безопасность
27. Организация конфиденциального делопроизводства
28. Защита информации в Интернете
29. Микроточки в стеганографии.
30. Методы классической стеганографии.
31. Криптография в истории. Интересные факты.
32. Тайны криптографии - нераскрытые шифры в истории.
33. Роторные шифровальные машины.
34. Методы ассиметричной криптографии.
35. Разновидности фишинга. Меры защиты.
36. Использование генераторов случайных чисел (в криптографии и не только).
37. Аппаратные и программные средства реализации криптографических методов.
38. Цифровые водяные знаки.
39. Мошенничество в социальных сетях.
40. Защита мобильных сетей.
41. Стеганография в истории, литературе, кинематографе.
42. Методы современного криптоанализа.

40. Защита мобильных сетей.
41. Стеганография в истории, литературе, кинематографе.
42. Методы современного криптоанализа.

ЗАДАНИЯ ПО КРИПТОГРАФИЧЕСКИМ МЕТОДАМ ЗАЩИТЫ

Задания по симметричной криптографии приведены в приложении 2

Задания по стеганографии приведены в приложении 3

ОПРОС НА СЕМИНАРСКИХ ЗАНЯТИЯХ

Образцы вопросов к семинарским занятиям приведены в приложении 4

Шкалы оценивания приведены в приложении 5

5.4. Перечень видов оценочных средств

Тест

Презентация

Задания по криптографическим методам защиты

Опрос на семинарских занятиях

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год
Л1.1	Блинов А.М.	Информационная безопасность. Ч. 1.: Учеб. пособие	СПб.: Изд-во СПбГУЭФ 2010
Л1.2	В.П. Мельников, С.А. Клейменов, А.М. Петраков; под ред. С.А. Клейменова	Информационная безопасность и защита информации: Учеб. пособие для студ. высш. учеб. заведений	М.: Издательский центр "Академия" 2011
Л1.3	Т.Л. Партыка, И.И. Попов	Информационная безопасность: Учебное пособие	Москва .: ФОРУМ 2012
Л1.4	В.И. Ярочкин	Информационная безопасность: Учебник	Москва .: Академический Проект 2005
Л1.5	Шаньгин, В. Ф.	Информационная безопасность компьютерных систем и сетей: учеб. Пособие	М.: ИД «ФОРУМ»: ИНФРА-М, 2012

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год
Л2.1	Макаренко С.И.	Информационная безопасность: Учеб. пособие для студ. вузов	Ставрополь: СФ МГГУ им. М.А. Шолохова 2009
Л2.2	Филин С.А.	Информационная безопасность: Учеб. пособие	М.: Издательство "Альфа-Пресс" 2010

6.1.3. Методические разработки

	Авторы, составители	Заглавие	Издательство, год
Л3.1	Завгородний В.И.	Комплексная защита информации в компьютерных системах: Учебное пособие	М.: Логос 2011
Л3.2	Степанов Е.А., Корнеев И.К.	Информационная безопасность и защита информации: Учебное пособие	М.: ИНФРА-М 2013

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	Введение в информационную безопасность. Основные понятия.	http://go.mail.ru/redir?q=%D0%92%D0%B2%D0%
Э2	Криптографические методы защиты информации.	http://go.mail.ru/redir?q=%D0%9A%D1%80%D0%
Э3	Вредоносные программы	http://go.mail.ru/redir?q=%D0%92%D1%80%D0%
Э4	Средства защиты сети.	http://go.mail.ru/redir?q=%D0%A1%D1%80%D0%
Э5	Социальный инжиниринг.	http://go.mail.ru/redir?q=%D1%81%D0%BE%D1%

6.3. Перечень информационных и образовательных технологий

6.3.1 Компетентностно-ориентированные образовательные технологии

6.3.1.1	Традиционные образовательные технологии – лекции, семинары, ориентированные прежде всего на сообщение знаний и способов действий, передаваемых студентам в готовом виде и предназначенных для воспроизводящего усвоения и разбора конкретных образцов.

6.3.1.2	Инновационные образовательные технологии – занятия в интерактивной форме, которые формируют системное мышления и способность генерировать идеи при решении различных творческих задач. К ним относятся электронные тексты лекций с презентациями, работа с аудио, видео материалами, работа в малых группах ,дискуссия.
6.3.1.3	Информационные образовательные технологии – самостоятельное использование студентом компьютерной техники и интернет-ресурсов для выполнения практических заданий и самостоятельной работы, создание лекций-презентаций, использование аудио-, видео- технические средства
6.3.2 Перечень информационных справочных систем и программного обеспечения	
6.3.2.1	операционная система Microsoft Windows 7-10, пакет прикладных программ Microsoft Office 2007-2010
6.3.2.2	программы для стеганографии FoxSecret и OpenPuff
6.3.2.3	учебно-методические комплексы по разделам дисциплины, размещенные на серверах компьютерных классов ФМО.

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)	
7.1	Лекционная аудитория с интерактивной доской на 60 посадочных мест (Ильбирс, ауд.402);
7.2	Компьютерные классы (Гл. корпус, ауд.315 и Ильбирс,ауд.411, 409) для выполнения практических занятий и самостоятельной работы.
7.3	.

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

ТЕХНОЛОГИЧЕСКАЯ КАРТА ДИСЦИПЛИНЫ в Приложении 6

МОДУЛЬНЫЙ КОНТРОЛЬ ПО ДИСЦИПЛИНЕ ВКЛЮЧАЕТ:

1. Текущий контроль: усвоение учебного материала на аудиторных занятиях (лекциях, практических, занятиях, в том числе учитывается посещение и активность) и выполнение обязательных заданий для самостоятельной работы
2. Рубежный контроль: проверка полноты знаний и умений по материалу модуля в целом. Выполнение модульных контрольных заданий проводится в письменном виде и является обязательной компонентой модульного контроля. К выполнению РК студент допускается всегда, независимо от посещаемости и выполнения других видов учебной работы.
3. Промежуточный контроль - завершенная задокументированная часть учебной дисциплины (или вся дисциплина полностью) – совокупность тесно связанных между собой зачетных модулей.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ВЫПОЛНЕНИЮ САМОСТОЯТЕЛЬНЫХ РАБОТ СТУДЕНТОВ

1. Советы по планированию и организации времени, необходимого для изучения дисциплины. Рекомендуется следующим образом организовать время, необходимое для изучения дисциплины:
Изучение конспекта лекции в тот же день, после лекции – 10-15 минут.
Изучение конспекта лекции за день перед следующей лекцией – 10-15 минут.
Изучение теоретического материала по учебному пособию и конспекту – 1 час в неделю.
Подготовка к практическому занятию – 2-3 час.
Всего в неделю – 4 часа.
2. Описание последовательности действий студента
Для понимания материала и качественного его усвоения рекомендуется такая последовательность действий:
1. После прослушивания лекции и окончания учебных занятий, при подготовке к занятиям следующего дня, нужно сначала просмотреть и обдумать текст лекции, прослушанной сегодня (10-15 минут).
2. При подготовке к лекции следующего дня, нужно просмотреть текст предыдущей лекции, подумать о том, какая может быть тема следующей лекции (10-15 минут).
3. В течение недели выбрать время (2-3часа) для работы с рекомендуемыми электронными учебными пособиями.
4. При подготовке к практическим занятиям следующего дня, необходимо сначала прочитать основные понятия и подходы по теме домашнего задания. При выполнении упражнения или задачи нужно сначала понять, что требуется в задаче, какой теоретический материал нужно использовать, наметить план решения задачи.
3. Рекомендации по использованию материалов учебно-методического комплекса. Все рекомендуемые учебные пособия размещены на серверах компьютерных классов ФМО в сетевой папке Мо на Teacher.
Рекомендуемые учебные пособия находятся в папке Информационная безопасность, а именно:
электронные учебники: 1) E-book_Фейгин_Информационная безопасность
4. Рекомендации по работе с литературой. Теоретический материал курса становится более понятным, когда дополнительно к прослушиванию лекции и изучению конспекта, изучаются и книги. Легче освоить курс, придерживаясь одного учебника и конспекта. Рекомендуется, кроме «заучивания» материала, добиться состояния понимания изучаемой темы дисциплины. С этой целью рекомендуется после изучения очередного параграфа выполнить несколько простых упражнений на данную тему. Кроме того, очень полезно мысленно задать себе следующие вопросы (и попробовать ответить на них): о чем этот параграф?, какие новые понятия введены, каков их смысл?, что даст это на практике?.
5. Советы по подготовке к рубежному и промежуточному контролям.
Рубежный контроль проходит в виде тестов, контрольных и самостоятельных работ.
Промежуточный контроль по данной дисциплине проходит в виде экзамена.

Дополнительно к изучению конспектов лекции необходимо пользоваться учебником.
При подготовке к промежуточному контролю нужно изучить теорию: определения всех понятий и подходы к оцениванию до состояния понимания материала и самостоятельно решить несколько типовых задач из каждой темы. При решении задач всегда необходимо уметь качественно интерпретировать итог решения.
6. Указания по организации работы с контрольно-измерительными материалами, по выполнению домашних заданий. При выполнении домашних заданий необходимо сначала прочитать основные понятия и подходы по теме задания. При выполнении упражнения или задачи нужно сначала понять, что требуется в задаче, какой теоретический материал нужно использовать, наметить план решения задачи, а затем приступить к расчетам и сделать качественный вывод.

Приложение 1

Примеры тестовых заданий по темам дисциплины Информационная безопасность:

Тема 1. Введение в информационную безопасность

Среди ниже перечисленных выделите главную причину существования многочисленных угроз информационной безопасности:
использование недостаточно апробированных технологий
архитектурные просчеты при построении информационных систем
использование приложений, полученных из ненадежных источников
Модификация информации, отрицание ее подлинности и/или навязывание ложной информации является нарушением
целостности
доступности
конфиденциальности
Расставьте угрозы информационной безопасности в порядке убывания финансовых потерь, к которым они приводят (начиная с самых больших потерь)
Хакеры
Вирусы, вредоносные программы
Кражи ноутбуков, КПК и других носителей информации
Инсайдеры и внутренние пользователи

Тема 2. Принципы построения защищенной АИС

Стандарты в области защиты информации относятся к мерам защиты
административным
законодательным
программно-техническим
процедурным
Согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов, называется
открытостью
гибкостью
комплексностью
системностью
Сложность обеспечения информационной безопасности является следствием:
невнимания широкой общественности к данной проблематике
все большей зависимости общества от информационных систем
быстрого прогресса информационных технологий, ведущего к постоянному изменению информационных систем и требований к ним

Темы 3-4. Симметричная криптография

Машина «Энигма» использовалась во время
Первой мировой войны
Второй мировой войны
Войны во Вьетнаме
Недостатки н-граммных шифров: (несколько правильных вариантов)
Меньшая криптостойкость, по сравнению с простой заменой

Больший объем таблицы замен
Сложнее для реализации
Укажите правильный порядок действий при частотном криптоанализе
сопоставление наиболее часто встречающимя знакам шифротекста часто встречающихся букв языка
подсчет количества повторяющихся знаков шифротекста
оценивается возможность сочетания тех или иных букв
В шифре Вижинера для алфавита из N символов используется подматрица шифрования размерностью:
•NxN
•2xN
•N^2xN^2
Поточные шифры различаются между собой
•Количеством раундов
•Размером ключа
•Способом построения генератора ключей
Исходный алфавит содержит следующие символы:
А Б В Г Д Е Ё Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я
Зашифруйте методом Вижинера слово УНИВЕР с ключом ДА
Соответствующая подматрица шифрования:
А Б В Г Д Е Ё Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я
Д Е Ё ЖЗ И Й К Л М НО П Р С Т У Ф ХЦ Ч ШЩЪЫ Ь Э ЮЯ А Б В Г
•ЧНМВЕР
•ЧЕМПИР
•ЧНМВИР

Тема 5. Стеганография и парольная защита

Желтые точки используются в
Принтерах
Сканерах
Фото и видео аппаратуре
Аналогом ЦВЗ можно считать понятия: (укажите несколько правильных вариантов ответа)
метки
заметки
лейбла
пояснения
Количество доступных для составления паролей символов на клавиатуре примерно равно
50
100
200

Тема6. Вредоносные программы

Большинство сетевых червей являются
резидентами
нерезидентами
В чём могут выражаться действия вируса?(укажите несколько правильных вариантов ответа)
заражение других программ

самостоятельное движение мышки по столу
замыкание проводки внутри системного блока
выдача ложных сообщений
выполнение функций, не предусмотренных программой: форматирование жёсткого диска, удаление и кодирование данных на диске
Для того, чтобы удалить вирус вручную, нужно
одеть перчатки
отключить сетевые подключения
загрузиться в безопасном режиме
это невозможно

Тема7. Средства защиты сети

Межсетевой экран выполняет функции:
•ускорения обмена информацией
•замедления обмена информацией
•протоколирования обмена информацией
Для обеспечения безопасности передачи данных в VPN используются
•картографические методы
•криптографические методы
•методы физической защиты
•стеганографические методы
Минимизация привилегий доступа подразумевает (укажите несколько правильных вариантов ответа)
• такое распределение ролей и ответственности, чтобы один человек не мог нарушить критически важный для организации процесс или создать брешь в защите по неведению или заказу злоумышленников.
•выделение пользователям и администраторам только тех прав доступа, которые необходимы им для выполнения служебных обязанностей
•привилегии распределяются между минимальным количеством людей

Тема8. Социальный инжиниринг

Обязаны ли вы сообщать свой пароль системным администраторам по их просьбе или требованию?
Нет
Да

Вы обязаны сообщать свой пароль:

администраторам сети
правоохранительным органам по требованию суда
родным и близким

К приемам фишинга можно отнести

заманивание на подставной сайт
телефонные звонки от имени системного администратора с требованием/просьбой сообщить пароль
атака на менее защищенный ресурс с целью получить доступ к более серьезным ресурсам
подсматривание в вашу записную книжку или сотовый

Приложение 2

Практические задания по симметричной криптографии

Исходный алфавит содержит следующие символы:
АБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ

1. Зашифруйте шифром Цезаря слово Интернет (ключ к=3)
2. Расшифруйте шифром Цезаря указанный текст (ключ к=5)

ЫКМЕХБ

3. Имеется таблица замены для двух шифров простой замены: шифра №1 и шифра №2.

Откр. текст	Шифр 1	Шифр 2		Откр. текст	Шифр 1	Шифр 2		Откр. текст	Шифр 1	Шифр 2
А	В	^		М	Т	№		Ч	М	∑
Б	И	@		Н	Ц	#		Ш	У	∇
В	О	)		О	.	-		Щ	Д	ϒ
Г	А	+		П	Ж	=		Ъ	Э	ℵ
Д	Щ	<		Р	Г	(		Ы	Н	⊕
Е	П	>		С	Л	?		Ь	Ю	×
Ж	К	∀		Т	Х	%		Э	Ы	ω
З	Б	♦		У	С	⊗		Ю	Ш	$
И	Ъ	*		Ф	Ь	!		Я	Е	Δ
К	пробел	♥		Х	Ч	№		пробел	Ф	∞
Л	Р	♠		Ц	З	®		.	Я	♣

Расшифруйте сообщения, зашифрованные с помощью шифра №1

a. И.РЮУ.ЪФОБГНО
b. СЛХГ.ЪЛХО.ФОО.ЩВ

Расшифруйте сообщения, зашифрованные с помощью шифра №2:

c. ∇*!(∞♦∧№>#⊕
d. @♠-♥∞∇*!(-)∧#*Δ

4. Известно, что при использовании шифра пропорциональной замены каждой русской букве поставлено в соответствие одно или несколько трехзначных чисел по таблице замен:

Таблица замен для пропорционального шифра										
Символ	Варианты замены				Символ	Варианты замены				
А	760	128	350	201	С	800	767	105		
Б	101				Т	759	135	214		
В	210	106			У	544				
Г	351				Ф	560				
Д	129				Х	768				
Е	761	130	802	352	Ц	545				
Ж	102				Ч	215				
З	753				Ш	103				
И	762	211	131		Щ	752				
К	754	764			Ъ	561				

Л	132	354				Ы	136					
М	755	742				Ь	562					
Н	763	756	212			Э	750					
О	757	213	765	133	353	Ю	570					
П	743	766				Я	216	104				
Р	134	532				Пробел	751	769	758	801	849	035…

Расшифруйте указанные сообщения.

`3532147641341367591367628497541282123503540357671062167532 11`

5. С помощью частотного криптоанализа расшифруйте название одного из методов шифрования:

(название состоит из двух слов, первые буквы в обоих словах зашифрованы шифром Цезаря)

Т Ъ Δ § _ $ ω Т Δ (§ _ $) Δ * + $

1. Пусть исходный алфавит содержит следующие символы:

АБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ

Зашифруйте с помощью шифра Вижинера и ключа КЛЮЧ сообщение:

- ШИФРОВКА

(используйте файл шифр.xls в папке Информационная безопасность)

2. Пусть исходный алфавит состоит из следующих знаков (символ "_" (подчеркивание) будем использовать для пробела):

АБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ_

Расшифруйте сообщения, зашифрованные с помощью шифра Вижинера и ключа OPEX:

- ЯБХЪШЮМХ

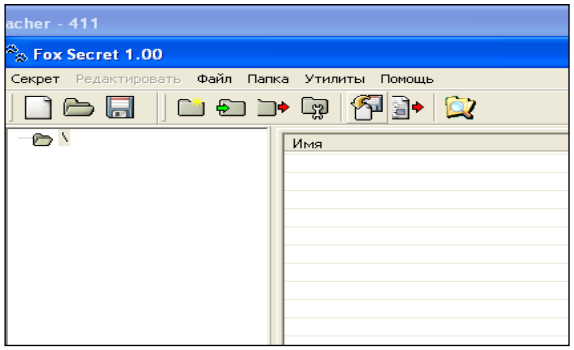
3. Зашифруйте методом перестановки с фиксированным периодом d=6 с ключом 436215 сообщения:
   - ЖЕЛТЫЙ_ОГОНЬ
   - МЫ_НАСТУПАЕМ
4. Расшифруйте сообщения, зашифрованные методом перестановки с фиксированным периодом d=8 с ключом 64275813:
   - СЛПИЬНАЕ
   - РОИАГДВН
5. Определите ключи в системе шифрования, использующей перестановку с фиксированным периодом d=5 по парам открытых и зашифрованных сообщений:
   - МОЙ ПАРОЛЬ – ЙПМ ООЬАЛР
   - СИГНАЛ БОЯ – НИСАГО ЛЯБ
6. Зашифруйте сообщения методом перестановки по таблице 5*5. Ключ указывает порядок считывания столбцов при шифровании.
   - ШИРОКОПОЛОСНЫЙ УСИЛИТЕЛЬ (ключ: 41235)
   - ПЕРЕДАЧА ИЗОБРАЖЕНИЯ (ключ: 24513)
7. Расшифруйте сообщения, зашифрованные методом перестановки по таблице 4*3. Пробелы пропущены. Ключ указывает порядок считывания столбцов при шифровании.
   - асасыгбиллйн(ключ: 3142)
8. Расшифруйте сообщения, зашифрованные методом перестановки по таблице 4*4 (символ подчеркивания заменяет пробел). Ключ указывает порядок считывания столбцов при шифровании.
   - еазапд_кеаурчв (ключ: 2143)
9. Расшифруйте сообщение, если известно, что оно зашифровано **двойным** циклом, каждый из которых содержит подстановку по Цезарю (ключ 3) и перестановку с ключом 35214.

Исходный алфавит АБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ

Криптограмма: КЭЖЖЩ

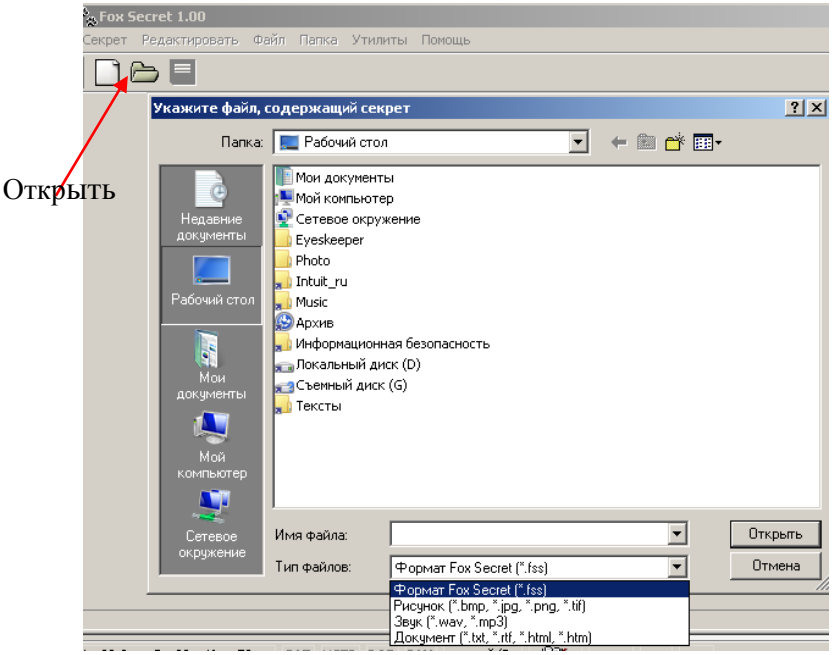
Практические задания по стеганографии

1. В **свою** папку **скопируйте** папку с файлами для распознавания - **Мо на Teacher/Информационная безопасность/Stego_задания.** Установите режим просмотра **Эскизы** и попытайтесь определить на глаз, в каких файлах есть вложения, в каких нет.



2. Убедившись, что это бесполезно, установите программу **FoxSecret** на свой ПК.
Для этого скопируйте в свою папку установочный файл **fs_setup_ru,** который находится в папке **Мо на Teacher/Информационная безопасность/Программы**.

- Запустите файл **fs_setup_ru** и пройдите все шаги установки. После окончания установки запустите программу через ярлык на Рабочем столе.



2. С помощью программы **FoxSecre**t:
2.1. Из 6 файлов (с именами **1,2,3,4,5,6**) из папки **Stego_задания** определите файлы с "**добавкой**" (вложениями). Извлеките "добавку"в свою папку. Выпишите в тетрадь файлы и вложения в виде таблицы:

Имя файла	Вложения
1	-
2	Текстовое сообщение

……
По умолчанию открываются файлы формата .**fss** (свой формат программы **FoxSecret**). Чтобы увидеть другие файлы, из списка для поля **Тип файлов** выбирайте по очереди другие варианты.

2.2. В один музыкальный файл (любой) поместите два вложения – картинку и текст. Музыку и картинку можно взять из **Мо на Teacher/Power-Point.**

Скопируйте музыкальный файл в свою папку и переименуйте его в ***Контейнер для 2_2***

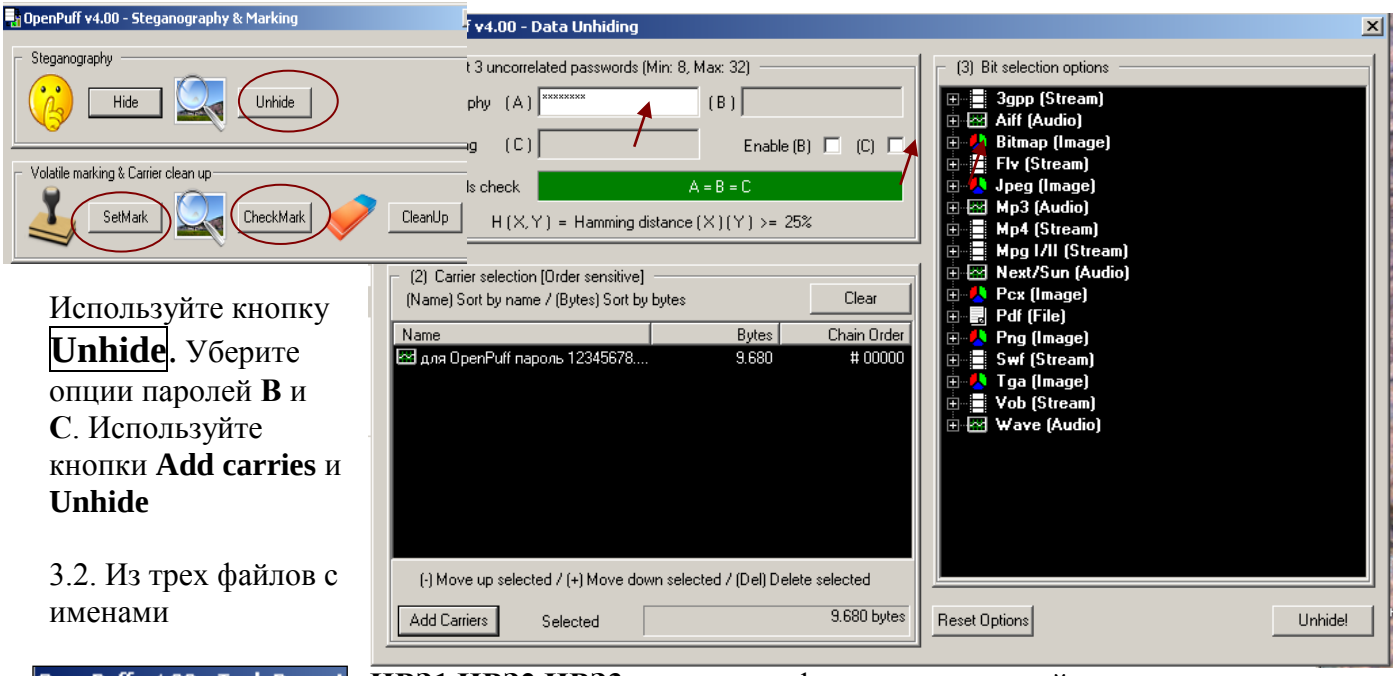
Скопируйте картинку в свою папку и переименуйте ее в ***Картинка для 2_2***

Создайте текстовый или word' файл сами и назовите его ***Текст для 2_2***

В программе **FoxSecret** используйте кнопку **Создать** и вариант **Сейф.** На втором шаге укажите вариант **Звук.** Далее укажите звуковой файл - ***Контейнер для 2_2*** из вашей папки**.** Без пароля идите вперед. Далее используйте кнопку **Добавить.** При закрытии программы не забудьте сохранить.

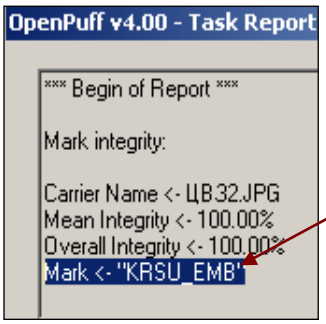
3. Программа **OpenPuff**.
Скопируйте папку **Информационная безопасность/Программы/OpenPuff** в свою папку и запустите файл **OpenPuff** .
С помощью программы OpenPuff:

3.1. Проверьте файл "**для OpenPuff пароль 12345678**" на наличие вложений.



Используйте кнопку **Unhide**. Уберите опции паролей **B** и **C**. Используйте кнопки **Add carries** и **Unhide**

3.2. Из трех файлов с именами



ЦВ31,ЦВ32,ЦВ33 определите фирменные, т.е. действительно имеющие ЦВЗ. Используйте кнопку **CheckMark.** Выпишите тексты ЦВЗ. Текст ЦВЗ находится в строке Mark.

3.3. Для любого мультимедийного или графического файла сделайте свой ЦВЗ. Кнопка **SetMark**. При сохранении укажите папку, отличную от той, где вы взяли картинку (в тот же самый файл программа не сохраняет).

Приложение 4

Образцы вопросов к семинарским занятиям

Тема 1 Введение в информационную безопасность

1. Основные понятия:
- конфиденциальность
- целостность
- доступность
- аутентичность
- апеллируемость
2. Угрозы информационной безопасности
- определение угрозы, атаки, нарушения
- классификация угроз
- естественные и искусственные, преднамеренные/непреднамеренные
- примеры часто встречающихся угроз
3. Основные принципы построения систем защиты АИС
- простота - непрерывность
- разумная достаточность - открытость

Тема 2 Принципы построения защищенной АИС

1. Задачи системы информационной безопасности
2. Меры противодействия угрозам безопасности
- законодательные
- административные
- политика безопасности
- процедурные
- программно-технические
3. Каналы утечки информации
4. Неформальная модель нарушителя
5. Информационная безопасность на уровне государства

Тема 3 Криптография I

- Перечислите методы защиты секретной информации
- Дайте определения криптографии, криптоанализу, криптологии, криптостойкости
- Области применения криптографии в современном обществе
- Поясните шифрование с помощью квадрата Полибия
- Что такое черные кабинеты, где и когда они появились
- В чем разница между кодированием и шифрованием
- На какие группы делятся все алгоритмы шифрования
- Поясните принципы симметричного шифрования
- Классификация методов симметричного шифрования
- Что значит одноалфавитная замена
- Что такое частотный анализ
- Особенности пропорциональных шифров

Как догадаться на каком языке (русском, английском, киргизском) написана криптограмма?

Тема 4 Криптография II

- Шифр Вижинера
- Преимущества многоалфавитных шифров
- Простая перестановка
- Перестановка по таблице
- Типы криптографических атак
- Атаки на основе известного и выбранного открытого текста
- Комбинированные методы шифрования, их преимущества
- Блочные шифры
- Поточные шифры
- Стандарты симметричных алгоритмов
- Проблемы симметричного шифрования
- Реализация криптографических методов

Можно ли в Кыргызстане использовать для криптографии шифр Цезаря?

Тема 5 Стеганография и парольная защита

- Определение стеганографии
- Классификация стеганографии
- Методы классической стеганографии
- Компьютерная стеганография
- Цифровая стеганография, ее методы
- Метод LSB
- ЦВЗ
- Применение стеганографии
- Роль парольной защиты
- Способы атаки на пароль
- Меры противодействия атакам на пароль

Тема 6 Компьютерные вирусы и борьба с ними

1. Общие сведения о компьютерных вирусах
2. Классификация вирусов
   - Особенности алгоритма
   - Деструктивные возможности
   - Среда обитания
3. Файловые вирусы
4. Макровирусы
5. Сетевые черви
6. Загрузочные вирусы
7. Троянские кони
8. Технологии маскировки вирусов
9. Тенденции современных компьютерных вирусов
10. Борьба с вирусами

Тема 7 Средства защиты сети.

1. Межсетевые экраны

- Назначение
- **Proxy-server**
- Классификация межсетевых экранов:

Проактивная защита

- Поведенческий контроль
- Режимы работы

Сравнительный анализ различных Firewalls

2. Виртуальные частные сети
- Определение
- Туннель
- Основные классы VPN
- Классификация VPN по архитектуре технического решения
- Классификация VPN по способу технической реализации

3. Системы обнаружения вторжений
- Назначение
- Структура СОВ

4. DoS-атаки
DoS-атака, определение.
DDoS-атака
Виды DoS-атак
- Ошибка
- Недостаточная проверка данных пользователя
- Флуд
- Атака второго рода

Выявление DoS-атак
Меры защиты
- Предотвращение.
- Фильтрация и блэкхолинг.
- Обратный DDOS.
- Наращивание ресурсов.
- Рассредоточение.
- Уклонение.
- Активные ответные меры.
- Использование оборудования для отражения DoS-атак.
- Приобретение сервиса по защите от DoS-атак.

Тема 8 Социальная инженерия
Области применения СИ
1) Три кита СИ:
i) Телефон
ii) Итернет
iii)Риаллайф (Real Life)
2) Искусство перевоплощения – модели поведения:
i) Начальник
ii) Секретарь
iii)Техслужащий
iv)Пользователь ПК
3) Приемы НЛП:
i) Доверчивость
ii) Жадность
iii)Страх
iv)Сопереживание (отзывчивость)
v) превосходство

Приложение 5

Шкалы оценивания

ШКАЛА ОЦЕНИВАНИЯ ТЕСТА

Наименование показателя	Баллы
Правильный ответ	3-5%
Не правильный ответ	0
Количество тестовых заданий	20-30
Всего	Сумма баллов

ШКАЛА ОЦЕНИВАНИЯ ЗАДАНИЙ ПО КРИПТОГРАФИИ

Наименование показателя	Баллы
Всего заданий 14	
Каждое задание	0-7 %
Всего	Сумма баллов

ШКАЛА ОЦЕНИВАНИЯ ЗАДАНИЙ ПО СТЕГАНОГРАФИИ

Наименование показателя	Баллы
Задание 1	0-15 %
Задание 2	0-25 %
Задание 3	0-30 %
Задание 4	0-15 %
Задание 5	0-15 %
Всего	Сумма баллов

ШКАЛА ОЦЕНИВАНИЯ ОТВЕТОВ НА СЕМИНАРСКИХ ЗАНЯТИЯХ

0-30%	31-59%	61-70%	71-84%	85-100%
Очень короткий ответ, или ответ не по существу заданного вопроса	Ответ прочитан по конспекту или по электронному учебнику	Ответ по существу вопроса, но без аргументации и объясняющих примеров	Ответ достаточно подробный, но затрудняется ответить на дополнительные (расширяющие тему) вопросы	Ответ подробный, с аргументацией и объясняющими примерами, отвечает на дополнительные, (расширяющие тему) вопросы

ШКАЛА ОЦЕНИВАНИЯ ПРЕЗЕНТАЦИИ

Наименование показателя	Баллы
Содержание	
• Полнота раскрытия темы презентации	0-25%

• Самостоятельность выполнения работы	0-25%
Оформление	
• Размещение текста и графических элементов	0-20%
• Эффекты анимации, смена слайдов	0-10%
• Наличие диаграмм и / или графиков	0-10%
• Шаблон оформления (фон)	0-5%
• Клип	0-5%
Всего	Сумма баллов

Приложение 6

Технологическая карта дисциплины

Название модулей дисциплины согласно РПД	Контроль	Форма контроля	Зачетный минимум	Зачетный максимум	График контроля
Модуль 1					
Введение в информационную безопасность. Криптография	Текущий контроль	Посещаемость (за каждое пропущенное и неотработанное занятие снимается 0,5 балла), СРС по темам: Способы раскрытия преступлений в сфере компьютерной информации. Хакеры и хакерское сообщество. Ассиметричная криптография Альтернативы алгоритму RSA Микроточки в стеганографии	7	10	11
	Рубежный контроль	Задания по криптографии и стеганографии Тестирование	15	25	
Модуль 2					
Антивирусная защита. Средства защиты сети. Социальный инжиниринг	Текущий контроль	Посещаемость (за каждое пропущенное и неотработанное занятие снимается 0,5 балла), СРС по темам: История появления вирусов и антивирусных программ Меры противодействия фишингу. Подготовка к круглому столу. Создание презентаций	8	15	17
	Рубежный контроль	Тестирование	10	20	
ВСЕГО за семестр			40	70	
Промежуточный контроль (Зачет)			20	30	
Семестровый рейтинг по дисциплине			60	100	