ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Директор института
Высшая школа экономики и управления

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Савельева И. П.
Пользователь: savelevaip
Дата подписания: 25.11.2019

И. П. Савельева

РАБОЧАЯ ПРОГРАММА
к ОП ВО от 26.06.2019 №084-2528

дисциплины Б.1.34 Информационная безопасность таможенных органов
для специальности 38.05.02 Таможенное дело
уровень специалист **тип программы** Специалитет
специализация Организация таможенного контроля
форма обучения очная
кафедра-разработчик Таможенное дело

Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 38.05.02 Таможенное дело, утверждённым приказом Минобрнауки от 17.08.2015 № 850

Зав.кафедрой разработчика,
к.экон.н., доц.

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Степанов Е. А.
Пользователь: stepanovea
Дата подписания: 20.11.2019

Е. А. Степанов

Разработчик программы,
к.экон.н., доцент

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Антоненко Е. В.
Пользователь: antonenkoev
Дата подписания: 20.11.2019

Е. В. Антоненко

Челябинск

1. Цели и задачи дисциплины

Цель изучения дисциплины — получить базовые знания в области защиты информации, хранящейся на рабочих станциях и серверах таможенных органов, подключенных к сети Интернет, а также при ее передаче по открытым каналам Интернет. Задачи изучения дисциплины: • освоение практических приемов защиты рабочих станций и серверов в таможенных органах; • получение навыков проектирования программно защищенных каналов передачи информации в системе таможенных органов.

Краткое содержание дисциплины

Защищенность информационной среды таможни — одно из основных условий ее эффективного функционирования. Комплекс мероприятий по обеспечению информационной безопасности информационной среды должен быть неотъемлемой частью системы управления таможенного органа. В настоящее время, персональные компьютеры (рабочие станции), как правило, подключены к глобальной сети Интернет. Знания и умения пользователя по обеспечению информационной безопасности персонального компьютера, работающего в сетевой среде внешней торговли, становятся одними из самых востребованных и необходимых. Данная дисциплина обеспечивает знакомство студента с теоретическими основами криптографии, инструментальными средствами и стандартами, поддерживающими разработку криптографического обеспечения информационных систем, практическими приемами защиты рабочих станций и серверов.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине (ЗУНы)
ОПК-3 способностью владеть методами и средствами получения, хранения, обработки информации, навыками использования компьютерной техники, программно-информационных систем, компьютерных сетей	Знать:потенциальные угрозы безопасности компьютерных систем; сервисы безопасности в таможенных органах;
	Уметь:настраивать почтовые сервисы для обеспечения конфиденциальности электронной переписки;
	Владеть:программными средствами реализации сервисов конфиденциальности;
ПК-32 владением навыками применения в таможенном деле информационных технологий и средств обеспечения их функционирования в целях информационного сопровождения профессиональной деятельности	Знать:проблемы при реализации систем безопасности; основные правила обеспечения безопасности рабочих станций и серверов;
	Уметь:обеспечивать конфиденциальность и аутентичность при взаимодействии web-приложений;
	Владеть:программными средствами реализации сервисов целостности, аутентичности.

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ

Б.1.09 Информатика	Б.1.38 Взаимодействие таможни и бизнеса

Требования к «входным» знаниям, умениям, навыкам студента, необходимым при освоении данной дисциплины и приобретенным в результате освоения предшествующих дисциплин:

Дисциплина	Требования
Б.1.09 Информатика	уметь работать в глобальной сети Интернет, знать теорию баз данных и основы двоичного исчисления

4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 3 з.е., 108 ч.

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		7
Общая трудоёмкость дисциплины	108	108
Аудиторные занятия:	48	48
Лекции (Л)	16	16
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	32	32
Лабораторные работы (ЛР)	0	0
Самостоятельная работа (СРС)	60	60
Изучение государственного стандарта 28147-89	20	20
Изучение государственного стандарта Р34.10-2001	20	20
Изучение государственного стандарта Р34.11-94	20	20
Вид итогового контроля (зачет, диф.зачет, экзамен)	-	экзамен

5. Содержание дисциплины

№ раздела	Наименование разделов дисциплины	Объем аудиторных занятий по видам в часах			
		Всего	Л	ПЗ	ЛР
1	Основные понятия и термины, относящиеся к информационной безопасности. Характерные проблемы, связанные с безопасностью, при использовании компьютерных сетей. Классификация атак. Сервисы безопасности. Правила обеспечения безопасности рабочей станции.	12	4	8	0
2	Криптография. Основные понятия и термины. Алгоритмы симметричного шифрования. Факторы безопасности алгоритмов симметричного шифрования. Примеры алгоритмов симметричного шифрования и их программная реализация.	12	4	8	0
3	Криптография с открытым ключом. Термины. Основные требования к алгоритмам асимметричного шифрования. Способы использования алгоритмов с открытым ключом. При-меры алгоритмов с открытым ключом и их программная реализация.	12	4	8	0

4	Криптографические стандарты. Цифровые сертификаты. Иерархия центров авторизации. Серверные и клиентские сертификаты. Безопасные коммуникации.	12	4	8	0

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
1	1	Характерные проблемы, связанные с безопасностью, при использовании компьютерных сетей; Последствия слабой системы безопасности; Проблемы при реализации системы безопасности; Роль разработчика в построении безопасных приложений; Классификация атак; Сервисы безопасности.	2
2	1	Правила обеспечения безопасности рабочей станции; Выполнение обновлений операционной системы; Выполнение обновлений прикладных программ; Установка антивирусной программы и регулярное обновление антивирусных баз; Настройка персонального брандмауэра.	2
3	2	Криптография. Криптоанализ. Определения. Термины. Стеганография,примеры использования. Факторы безопасности алгоритмов симметричного шифрования. Абсолютно стойкий шифр.	2
4	2	Структура блочного алгоритма симметричного шифрования; Симметричное шифрование блока Алгоритмы DES, AES;	2
5	3	Основные требования к алгоритмам асимметричного шифрования (шифрования с открытым ключом). Терминология в алгоритмах асимметричного шифрования. Понятие односторонней функции с секретом. Правила модульной арифметики.	2
6	3	Способы использования алгоритмов с открытым ключом (зашифровывание/расшифровывание). Цифровая подпись (прямая, арбитражная)	2
7	4	Цифровые сертификаты Стандарт X.509. Спецификации PKI Иерархия центров авторизации цифровых сертификатов	2
8	4	Серверные и клиентские сертификаты. Безопасные ком-муникации на основе SSL.	2

5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-во часов
1,2	1	Настройка и проверка защищенности Internet коммуникаций	4
3,4	1	Использование и защита почтовых протоколов	4
5,6	2	Криптоанализ зашифрованного текста	4
7,8	2	Использование PGP и GPG для обеспечения конфиденциальности электронной почты и шифрования файлов	4
9,10	3	Использование PKI (инфраструктуры открытых ключей) для защиты электронной почты и web-коммуникаций в таможенных органах	4
11,12	3	Основные требования к алгоритмам асимметричного шифрования (шифрования с открытым ключом). Терминология в алгоритмах асимметричного шифрования. Понятие односторонней функции с секретом. Правила модульной арифметики.	4
13,14	4	Серверные и клиентские сертификаты. Безопасные коммуникации на базе SSL	4
15,16	4	Цифровые сертификаты Стандарт X.509. Спецификации PKI Иерархия	4

		центров авторизации цифровых сертификатов	

5.3. Лабораторные работы

Не предусмотрены

5.4. Самостоятельная работа студента

Выполнение СРС		
Вид работы и содержание задания	Список литературы (с указанием разделов, глав, страниц)	Кол-во часов
Изучение государственного стандарта 28147-89	http://protect.gost.ru/document.aspx?control=7&id=139177	20
Изучение государственного стандарта Р34.10-2001	http://protect.gost.ru/document.aspx?control=7&id=131131	20
Изучение государственного стандарта Р34.11-94	http://ru.wikipedia.org/wiki/%D0%93%D0%9E%D0%A1%D0%A2_%D0%A0_34.11-94	20

6. Инновационные образовательные технологии, используемые в учебном процессе

Инновационные формы учебных занятий	Вид работы (Л, ПЗ, ЛР)	Краткое описание	Кол-во ауд. часов
Разбор конкретных ситуаций	Лекции	Разбор и моделирование атаки “man in the middle” на примере электронной почты	3

Собственные инновационные способы и методы, используемые в образовательном процессе

Не предусмотрены

Использование результатов научных исследований, проводимых университетом, в рамках данной дисциплины: нет

7. Фонд оценочных средств (ФОС) для проведения текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

7.1. Паспорт фонда оценочных средств

Наименование разделов дисциплины	Контролируемая компетенция ЗУНы	Вид контроля (включая текущий)	№№ заданий

Все разделы	ПК-32 владением навыками применения в таможенном деле информационных технологий и средств обеспечения их функционирования в целях информационного сопровождения профессиональной деятельности	Экзамен	1
Основные понятия и термины, относящиеся к информационной безопасности. Характерные проблемы, связанные с безопасностью, при использовании компьютерных сетей. Классификация атак. Сервисы безопасности. Правила обеспечения безопасности рабочей станции.	ОПК-3 способностью владеть методами и средствами получения, хранения, обработки информации, навыками использования компьютерной техники, программно-информационных систем, компьютерных сетей	Текущий	3
Криптография. Основные понятия и термины. Алгоритмы симметричного шифрования. Факторы безопасности алгоритмов симметричного шифрования. Примеры алгоритмов симметричного шифрования и их программная реализация.	ОПК-3 способностью владеть методами и средствами получения, хранения, обработки информации, навыками использования компьютерной техники, программно-информационных систем, компьютерных сетей	Текущий	2
Криптография с открытым ключом. Термины. Основные требования к алгоритмам асимметричного шифрования. Способы использования алгоритмов с открытым ключом. Примеры алгоритмов с открытым ключом и их программная реализация.	ОПК-3 способностью владеть методами и средствами получения, хранения, обработки информации, навыками использования компьютерной техники, программно-информационных систем, компьютерных сетей	Текущий	4
Криптографические стандарты. Цифровые сертификаты. Иерархия центров авторизации. Серверные и клиентские сертификаты. Безопасные коммуникации.	ПК-32 владением навыками применения в таможенном деле информационных технологий и средств обеспечения их функционирования в целях информационного сопровождения профессиональной деятельности	Текущий	5
Все разделы	ОПК-3 способностью владеть методами и средствами получения, хранения, обработки информации, навыками использования компьютерной техники, программно-информационных систем, компьютерных сетей	Экзамен	1

7.2. Виды контроля, процедуры проведения, критерии оценивания

Вид контроля	Процедуры проведения и оценивания	Критерии оценивания
Экзамен	Решение теста Тестирование студенты осуществляют на занятии, на базе платформы Электронный ЮУрГУ. Студенту необходимо ответить на 25 тестовых вопросов. Время, отведенное на тестирование - 25 минут При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена	Отлично: 85% и более от максимального количества баллов Хорошо: от 75% до 85% от максимального количества баллов

	приказом ректора от 24.05.2019 г. № 179) Правильный ответ соответствует 1 баллу. Максимальное количество баллов = 25. Весовой коэффициент мероприятия = 1.	Удовлетворительно: от 60% до 75% от максимального количества баллов Неудовлетворительно: менее 60% от максимального количества баллов
Текущий	Тестирование. Тестирование студенты осуществляют на занятии, на базе платформы Электронный ЮУрГУ. Студенту необходимо ответить на 15 тестовых вопросов. Время, отведенное на тестирование - 25 минут При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179) Правильный ответ соответствует 1 баллу. Максимальное количество баллов = 25. Весовой коэффициент мероприятия = 1.	Отлично: 85% и более от максимального количества баллов Хорошо: от 75% до 85% от максимального количества баллов Удовлетворительно: от 60% до 75% от максимального количества баллов Неудовлетворительно: менее 60% от максимального количества баллов
Текущий	Тестирование. Тестирование студенты осуществляют на занятии, на базе платформы Электронный ЮУрГУ. Студенту необходимо ответить на 10 тестовых вопросов. Время, отведенное на тестирование - 20 минут При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179) Правильный ответ соответствует 1 баллу. Максимальное количество баллов = 25. Весовой коэффициент мероприятия = 1.	Отлично: 85% и более от максимального количества баллов Хорошо: от 75% до 85% от максимального количества баллов Удовлетворительно: от 60% до 75% от максимального количества баллов менее 60% от максимального количества баллов Неудовлетворительно: менее 60% от максимального количества баллов
Текущий	Тестирование. Тестирование студенты осуществляют на занятии, на базе платформы Электронный ЮУрГУ. Студенту необходимо ответить на 10 тестовых вопросов. Время, отведенное на тестирование - 20 минут При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179) Правильный ответ соответствует 1 баллу. Максимальное количество баллов = 25. Весовой коэффициент мероприятия = 1.	Отлично: 85% и более от максимального количества баллов Хорошо: от 75% до 85% от максимального количества баллов Удовлетворительно: от 60% до 75% от максимального количества баллов Неудовлетворительно: менее

		60% от максимального количества баллов
Текущий	Тестирование. Тестирование студенты осуществляют на занятии, на базе платформы Электронный ЮУрГУ. Студенту необходимо ответить на 10 тестовых вопросов. Время, отведенное на тестирование - 20 минут При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179) Правильный ответ соответствует 1 баллу. Максимальное количество баллов = 25. Весовой коэффициент мероприятия = 1.	Отлично: 85% и более от максимального количества баллов Хорошо: от 75% до 85% от максимального количества баллов Удовлетворительно: от 60% до 75% от максимального количества баллов Неудовлетворительно: менее 60% от максимального количества баллов

7.3. Типовые контрольные задания

Вид контроля	Типовые контрольные задания
Экзамен	1. Выберите верное утверждение. Информационная безопасность автоматизированной системы – это состояние автоматизированной системы, при котором она: a) с одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой — ее наличие и функционирование не создает информационных угроз для элементов самой системы и внешней среды; b) с одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой – затраты на её функционирование ниже, чем предполагаемый ущерб от утечки защищаемой информации c) способна противостоять только информационным угрозам, как внешним так и внутренним d) способна противостоять только внешним информационным угрозам. 2. Выберете верное утверждение. Атака «man in the middle» является: a) пассивной; b) активной; c) может быть как активной, так и пассивной; d) нет верных ответов. 3. Выберете верное утверждение. Целостность – это: a) невозможность несанкционированного просмотра информации; b) невозможность несанкционированного изменения информации; c) невозможность несанкционированного доступа к информации; d) невозможность несанкционированного получения информации. 4. Выберете верное утверждение. Аутентификация – это: a) невозможность несанкционированного просмотра информации; b) невозможность несанкционированной модификации информации; c) невозможность несанкционированного доступа к данным; d) подтверждение того, что информация получена из законного источника законным получателем. 5. Выберете верное утверждение. Наука о методах сокрытия самого факта передачи сообщения называется: a) криптологией;

b) криптоанализом;
c) криптографией;
d) стеганонографией.
6. Что из нижеперечисленного понимается под DoS-атакой:
a) модификация передаваемого сообщения;
b) повторное использование переданного ранее сообщения;
c) невозможность получения сервиса законным пользователем;
d) нет верных ответов.
7. Сервис, который обеспечивает невозможность несанкционированного просмотра данных, называется:
a) аутентификацией;
b) целостностью;
c) конфиденциальностью;
d) авторизацией.
8. Сервис, который гарантирует, что информация получена из законного источника и получателем является тот, кто нужно, называется:
a) аутентификацией;
b) целостностью;
c) конфиденциальностью;
d) авторизацией.
9. «Парадокс дня рождения» состоит в том, что:
a) для того, чтобы вероятность совпадения дней рождения у двух человек была больше 0.5, в группе должно быть всего 23 человека;
b) для того, чтобы вероятность совпадения дней рождения у двух человек была больше 0.5, в группе должно быть всего 32 человека;
c) для того, чтобы вероятность совпадения дней рождения у двух человек была равна 1, в группе должно быть всего 23 человека;
d) для того, чтобы вероятность совпадения дней рождения у двух человек была равна 1, в группе должно быть всего 23 человека.
10. Модификация передаваемого сообщения называется
a) DoS-атакой;
b) Replay-атакой;
c) атакой «man-in-the-middle»;
d) Фальсификацией.
11. Повторное использование переданного ранее сообщения называется
a) DoS-атакой;
b) Replay-атакой;
c) атакой «man-in-the-middle»;
d) фальсификацией.
12. Выберете верное утверждение. Наука о методах создания и анализа систем безопасной связи называется:
e) криптологией;
a) криптоанализом;
b) криптографией;
c) стеганонографией.
13. Алгоритм Диффи-Хеллмана основан на:
a) задаче линейного программирования
b) задаче дискретного логарифмирования;
c) задаче факторизации числа;
d) задаче определения, является ли данное число простым.
14. Выберете верный ответ. Каким термином называется исходное сообщение (файл, трафик, передаваемый между узлами сети и т.д.), которое должно быть защищено криптографическими методами?
a) передаваемый текст;
b) закрытый текст;
c) открытый текст;

d) шифруемый текст.
15. Криптоанализ – это процесс, при котором:
a) зная зашифрованное сообщение, пытаются узнать незашифрованное сообщение;
b) зная одну или несколько пар (незашифрованное сообщение, зашифрованное сообщение), пытаются узнать ключ
c) изменяют передаваемое зашифрованное сообщение;
d) +верны ответы a) и b).
16. Выберете верный ответ. Каким термином называется исходное сообщение (файл, трафик, передаваемый между узлами сети и т.д.), которое должно быть защищено криптографическими методами?
e) передаваемый текст;
f) закрытый текст;
g) открытый текст;
h) шифруемый текст.
17. Выберете верный ответ. Каким термином называется способность противостоять вооруженному современной техникой и знаниями противнику к раскрытию ключа, нарушению целостности и подлинности информации?
a) защита шифра;
b) нерушимость шифра;
c) стойкость шифра;
d) нет верных ответов.
18. Функция, которую можно использовать в криптосистеме с открытым ключом, должна обладать следующими свойствами:
a) не иметь обратной функции;
b) вычисление обратной функции должно иметь полиномиальную сложность без знания дополнительной информации;
c) +вычисление обратной функции должно иметь экспоненциальную сложность без знания;
d) дополнительной информации и полиномиальную сложность, если эта информация известна.
19. Аутентификация сторон в алгоритме Диффи-Хеллмана необходима, потому что:
a) +в противном случае атакующий может перехватить передаваемые открытые ключи и заменить их своим открытым ключом;
b) в противном случае атакующий может взломать дискретный логарифм;
c) в противном случае атакующий может взломать натуральный логарифм;
d) в противном случае стороны не смогут вычислить общий секрет.
20. Алгоритм Диффи-Хеллмана дает возможность
a) безопасно обменяться общим секретом;
b) безопасно обменяться общим секретом при условии аутентификации сторон;
c) подписать сообщение;
d) все ответы верны.
21. Подпись, создаваемая RSA, является:
a) детерминированной;
b) рандомизированной;
c) логарифмической;
d) дискретной.
22. Для создания подписи следует использовать
a) свой открытый ключ;
b) открытый ключ получателя;
c) закрытый ключ получателя;
d) +свой закрытый ключ.
23. Задачей дискретного логарифмирования является
a) разложение числа на простые сомножители;
b) нахождение степени, в которую следует возвести целое число для получения заданного целого числа;
c) нахождение степени, в которую следует возвести простое число для получения

	заданного целого числа; d) нет верных ответов. 24. Для каких целей используется алгоритм RSA? a) подписывания; b) шифрования; c) обмена общим секретом; d) +все ответы верны. 25. Зависимость между ключами шифрования и дешифрования в алгоритмах симметричного шифрования должна быть следующей: a) ключи шифрования и дешифрования должны в точности совпадать b) ключ дешифрования должен легко получаться из ключа шифрования c) между ключами шифрования и дешифрования не должно быть никакой зависимости d) Верны ответы a) и b). Экзамен.docx
Текущий	1. Выберете верный ответ. Каким образом называется эффективная стратегия осуществления атак, которые работают по выбранным открытым текстам? a) тотальное опробывание ключей; b) дифференциальный криптоанализ; c) линейный криптоанализ; d) программный криптоанализ. 2. Для шифрования сообщения следует использовать: a) свой открытый ключ; b) открытый ключ получателя; c) свой закрытый ключ; d) закрытый ключ получателя. 3. Криптоанализ – это процесс, при котором: a) зная зашифрованное сообщение, пытаются узнать незашифрованное сообщение; b) зная одну или несколько пар (незашифрованное сообщение, зашифрованное сообщение), пытаются узнать ключ c) изменяют передаваемое зашифрованное сообщение; d) верны ответы a) и b). 4. Криптографическая система называется симметричной, потому что a) шифруемый блок разбивается на подблоки одинаковой длины; b) для шифрования и дешифрования используются одинаковые или легко выводимые один из другого ключи; c) алгоритм использует циклически повторяющиеся операции, называемые раундами; d) нет верных ответов. 5. Задачей дискретного логарифмирования является a) разложение числа на простые сомножители; b) нахождение степени, в которую следует возвести целое число для получения заданного целого числа; c) нахождение степени, в которую следует возвести простое число для получения заданного целого числа; d) нет верных ответов. 6. Алгоритм симметричного шифрования называется блочным, если a) алгоритм основан на сети Фейстеля; b) для шифрования исходный текст разбивается на блоки фиксированной длины; c) в алгоритме используются S-box; d) все ответы верны. 7. Выберете верный ответ. Каким термином называется исходное сообщение (файл, трафик, передаваемый между узлами сети и т.д.), которое должно быть защищено криптографическими методами? a) передаваемый текст; b) закрытый текст; c) открытый текст; d) шифруемый текст.

	8. Выберете верный ответ. Каким термином называется способность противостоять вооруженному современной техникой и знаниями противнику к раскрытию ключа, нарушению целостности и подлинности информации? a) защита шифра; b) нерушимость шифра; c) стойкость шифра; d) нет верных ответов. 9. Выберете верное утверждение? Длина ключа алгоритма AES должна быть не меньше: a) 56 бит; b) 64 бита; c) 128 бит; d) 256 бит. 10. Зависимость между ключами шифрования и дешифрования в алгоритмах симметричного шифрования должна быть следующей: a) ключи шифрования и дешифрования должны в точности совпадать b) ключ дешифрования должен легко получаться из ключа шифрования c) между ключами шифрования и дешифрования не должно быть никакой зависимости d) Верны ответы a) и b). 11. Главным требованием к алгоритму, принимаемому в качестве стандарта AES, была: a) низкая стоимость алгоритма; b) простота алгоритма; c) эффективность выполнения алгоритма на различных архитектурах; d) безопасность алгоритма. 12. Алгоритм RC6 обладает следующими свойствами: a) имеет самое быстрое шифрование/дешифрование; b) имеет возможность вычисления подключей на лету; c) шифрование и дешифрование имеют идентичные функции; d) все ответы верны. 13. Алгоритм RC6 характеризуется следующими свойствами a) имеет длину блока 128 бит; b) основан на сети Фейстеля; c) использует S-boxes; d) верны ответы a) и b). 14. Выберете верный ответ. Каким образом называется эффективная стратегия осуществления атак, которые работают как по выбранным открытым текстам, так и по известным открытым текстам? e) тотальное опробывание ключей; a) дифференциальный криптоанализ; b) линейный криптоанализ; c) программный криптоанализ. 15. Какая должна быть длина ключа в алгоритме ГОСТ 28147? a) 56 бит; b) 128 бит; c) 256 бит; d) 448 бит. Крипто.docx
Текущий	1. Сопоставьте: А. Вирусы а. Используется для DDOS-атак Б. Черви б. Вредоносное ПО, которое выглядит законно В. Троян в. Автономное вредоносное ПО, способное саморазмножаться Г. Бот г. Распространяются путем внедрения своей копии в другую программу Ответ: Аг Бв Вб Га 2. Категория программного обеспечения, предназначенная для блокирования определенного вида сетевого трафика – это… А. Брандмауэр (FireWall) Б. Программа-шпион

	В. Антивирус Г. Нет верного ответа 3. Наука, занимающаяся методами шифрования и дешифрования – это … А. Криптография Б. Криптоанализ В. Криптология Г.Стеганография 4. Наука о преодолении криптографической защиты информации – это … А. Криптография Б. Криптоанализ В. Криптология Г.Стеганография 5. Сокрытие данных и самого факта их существования – это … А. Криптография Б. Криптоанализ В. Криптология Г.Стеганография 6. Совокупность заранее оговоренных способов преобразования исходного секретного сообщения с целью его защиты – это … А. Шифр Б. Открытый текст В. Криптограмма Г. Ключ 7. Исходное сообщение часто называют … А. Шифр Б. Открытый текст В. Криптограмма Г. Ключ 8. Сообщение, полученное после преобразования с использованием любого шифра – это … А. Шифр Б. Открытый текст В. Криптограмма Г. Ключ 9. Информация, необходимая для шифрования и расшифрования сообщений – это … А. Шифр Б. Открытый текст В. Криптограмма Г. Ключ 10. Процесс преобразования открытого текста в шифртекст с использованием ключа – это … А. Зашифрование Б. Расшифрование В. Дешифрование Г. Нет верного ответа
Текущий	1. Для каких целей используется алгоритм RSA? a) подписывания; b) шифрования; c) обмена общим секретом; d) все ответы верны. 2. Алгоритм Диффи-Хеллмана дает возможность a) безопасно обменяться общим секретом; b) безопасно обменяться общим секретом при условии аутентификации сторон; c) подписать сообщение; d) все ответы верны. 3. Подпись, создаваемая RSA, является:

	a) детерминированной; b) рандомизированной; c) логарифмической; d) дискретной. 4. Подпись, создаваемая DSS, является a) детерминированой; b) рандомизированной; c) логарифмической; d) полиморфной. 5. Функция, которую можно использовать в криптосистеме с открытым ключом, должна обладать следующими свойствами: a) не иметь обратной функции; b) вычисление обратной функции должно иметь полиномиальную сложность без знания дополнительной информации; c) вычисление обратной функции должно иметь экспоненциальную сложность без знания; d) дополнительной информации и полиномиальную сложность, если эта информация известна. 6. Мастер-ключ используется для: a) шифрования ключа сессии; b) шифрования прикладных данных; c) шифрования как ключа сессии, так и прикладных данных; d) нет правильных ответов. 7. Аутентификация сторон в алгоритме Диффи-Хеллмана необходима, потому что: a) в противном случае атакующий может перехватить передаваемые открытые ключи и заменить их своим открытым ключом; b) в противном случае атакующий может взломать дискретный логарифм; c) в противном случае атакующий может взломать натуральный логарифм; d) в противном случае стороны не смогут вычислить общий секрет. 8. При односторонней аутентификации осуществляется аутентификация a) отправителя; b) получателя; c) отправителя и получателя; d) нет верных ответов. 9. Атака, при которой противник принимает на себя идентичность одного из законных участников протокола, называется: a) атакой по известным ключам; b) атакой методом повторного сеанса; c) атакой методом персонификации; d) словарной атакой. 10. Атака путем перебора наиболее вероятных значений каких-либо величин или сообщений, используемых в протоколе называется: a) атакой по известным ключам; b) атакой методом повторного сеанса; c) атакой методом персонификации; d) словарной атакой.
Текущий	1. Участник криптосистемы, которому доверяют все ее абоненты, называется: a) центр сертификации ключей; b) сервер распознавания ключей; c) удостоверяющий ключевой центр; d) все ответы верны. 2. Хэш-функция должна обладать следующими свойствами: a) для любого данного значения хэш-кода h вычислительно невозможно найти M такое, что H (M) = h; b) хэш-функция H должна применяться к блоку данных фиксированной длины; c) хэш-функция H создает выход фиксированной длины;

	d) верны ответы a) и c) 3. Хэш-функция должна обладать следующими свойствами: a) H (M) относительно легко (за полиномиальное время) вычисляется для любого значения M; b) для любого данного x вычислительно невозможно найти y ≠ x, что H (y) = H (x); c) для любого данного x вычислительно невозможно найти H (x); d) верны ответы a) и b). 4. Хэш-функции предназначены для: a) сжатия сообщения; b) получения «отпечатков пальцев» сообщения; c) шифрования сообщения; d) дешифрования сообщения. 5. При односторонней аутентификации ключ сессии может шифроваться a) открытым ключом получателя; b) закрытым ключом отправителя; c) мастер-ключом для симметричного шифрования, разделяемым отправителем и KDC; d) Верны ответы a) и c). 6. Сильная хэш-функция отличается от слабой наличием следующего свойства: a) у сильной хэш-функции для любого данного значения хэш-кода h вычислительно невозможно найти M такое, что H (M) = h; b) у сильной хэш-функции вычислительно невозможно найти произвольную пару (x, y) такую, что H (y) = H (x); c) у сильной хэш-функции для любого данного x вычислительно невозможно найти y ≠ x, что H (y) = H (x); d) нет верных ответов. 7. Подпись называется детерминированной, если: a) для одного и того же сообщения с использованием разных закрытых ключей при каждом подписывании создается одна и та же подпись; b) для разных сообщений с использованием одного и того закрытого ключа при каждом подписывании создается одна и та же подпись; c) для одного и того же сообщения с использованием одного и того же закрытого ключа при каждом подписывании создается одна и та же подпись; d) для одного и того же сообщения с использованием открытого ключа при каждом подписывании создается одна и та же подпись. 8. Из каких полей должен состоять сертификат открытого ключа? a) поля данных; b) поля подписи; c) поля данных и поля подписи; d) нет верных ответов. 9. Подпись называется рандомизированной, если: a) для разных сообщений с использованием одного и того же закрытого ключа при каждом подписывании создаются разные подписи; b) для одного и того же сообщения с использованием одного и того же закрытого ключа при каждом подписывании создаются разные подписи; c) для одного и того же сообщения с использованием разных закрытых ключей при каждом подписывании создаются разные подписи; d) для одного и того же сообщения с использованием открытого ключа при каждом подписывании создается одна и та же подпись. 10. Каждый блок сообщения в хэш-функции MD5 обрабатывается a) 4 раза; b) 16 раз; c) 32 раза; d) 64 раза.

8. Учебно-методическое и информационное обеспечение дисциплины

Печатная учебно-методическая документация

а) основная литература:

1. Закиров, Р. Ш. Информационная безопасность Текст конспект лекций по направлениям подготовки "Экономика" и "Менеджмент" Р. Ш. Закиров ; Юж.-Урал. гос. ун-т, Каф. Экономика и упр. проектами ; ЮУрГУ. - Челябинск: Издательский Центр ЮУрГУ, 2014. - 72, [1] с. электрон. версия
2. Степанов, Е. А. Информационная безопасность и защита информации Учеб. пособие для вузов по специальности "Документоведение и документацион. обеспечение упр." Е. А. Степанов, И. К. Корнеев. - М.: ИНФРА-М, 2001. - 301,[1] с. ил.
3. Информатика Текст Т. 1 Концептуальные основы учебник по специальности 090106 "Информ. безопасность телекоммуникац. систем" авт.-ред. В. А. Минаев и др. - 2-е изд., расш. и доп. - М.: Маросейка, 2008. - 463 с. ил. 22 см.

б) дополнительная литература:

1. Суховилов, Б. М. Защита информации в корпоративных информационных системах Текст учеб. пособие к практ. работам по направлению "Приклад. информатика" Б. М. Суховилов ; Юж.-Урал. гос. ун-т, Каф. Информатика ; ЮУрГУ. - Челябинск: Издательский Центр ЮУрГУ, 2013. - 39, [1] с. ил. электрон. версия
2. Информатика Текст Т. 1 Концептуальные основы учебник по специальности 090106 "Информ. безопасность телекоммуникац. систем" авт.-ред. В. А. Минаев и др. - 2-е изд., расш. и доп. - М.: Маросейка, 2008. - 463 с. ил. 22 см.
3. Грушо, А. А. Теоретические основы компьютерной безопасности Текст учеб. пособие для вузов по специальности 090100 "Информационная безопасность" А. А. Грушо, Э. А. Применко, Е. Е. Тимонина. - М.: Академия, 2009. - 267, [1] с.

в) отечественные и зарубежные журналы по дисциплине, имеющиеся в библиотеке:

г) методические указания для студентов по освоению дисциплины:

1. Контрольные вопросы для подготовки к зачету

из них: учебно-методическое обеспечение самостоятельной работы студента:

2. Контрольные вопросы для подготовки к зачету

Электронная учебно-методическая документация

№	Вид литературы	Наименование разработки	Наименование ресурса в электронной форме	Доступность (сеть Интернет / локальная сеть; авторизованный / свободный доступ)
1	Основная литература	Малышенко, Ю.В. Таможенное декларирование и предварительное	Электронно-библиотечная	Интернет / Авторизованный

		информирование в электронной форме. [Электронный ресурс] — Электрон. дан. — СПб. : ИЦ Интермедия, 2012. — 326 с. — Режим доступа: http://e.lanbook.com/book/55342 — Загл. с экрана.	система издательства Лань	
2	Дополнительная литература	Сальников, К.А. Декларирование товаров и транспортных средств. [Электронный ресурс] — Электрон. дан. — СПб. : ИЦ Интермедия, 2015. — 228 с. — Режим доступа: http://e.lanbook.com/book/55326 — Загл. с экрана.	Электронно-библиотечная система издательства Лань	Интернет / Авторизованный

9. Информационные технологии, используемые при осуществлении образовательного процесса

Перечень используемого программного обеспечения:

1. Microsoft-Office(бессрочно)
2. ООО Альта-софт-Альта-Максимум (версия PRO)(бессрочно)
3. Microsoft-Windows(бессрочно)
4. -Microsoft Visual Studio (бессрочно)

Перечень используемых информационных справочных систем:

Нет

10. Материально-техническое обеспечение дисциплины

Вид занятий	№ ауд.	Основное оборудование, стенды, макеты, компьютерная техника, предустановленное программное обеспечение, используемое для различных видов занятий
Лекции	118 (3б)	20 компьютерных рабочих мест, 1 ноутбук, 1 проектор, 1 экран, 1 коммутатор, 1 доска магнитная маркерная. Досмотровый комплект зеркал «Поиск-2У», Комплект сменных щупов «КЩ-3М», Переносной комплект технических средств для обследования автотранспорта «Гастроль П», Портативный ультрафиолетовый осветитель «Дозор-В», Прибор для углубленной светооптической проверки документов «Генетика-02.01»; Экран Da-liteModel B 152x203. 7 парт со скамьей, 10 столов компьютерных, 1 стол письменный с тумбой, 20 стульев ИЗО.
Практические занятия и семинары	118 (3б)	20 компьютерных рабочих мест, 1 ноутбук, 1 проектор, 1 экран, 1 коммутатор, 1 доска магнитная маркерная. Досмотровый комплект зеркал «Поиск-2У», Комплект сменных щупов «КЩ-3М», Переносной комплект технических средств для обследования автотранспорта «Гастроль П», Портативный ультрафиолетовый осветитель «Дозор-В», Прибор для углубленной светооптической проверки документов «Генетика-02.01»; Экран Da-liteModel B 152x203. 7 парт со скамьей, 10 столов компьютерных, 1 стол письменный с тумбой, 20 стульев ИЗО.
Экзамен	118 (3б)	20 компьютерных рабочих мест, 1 ноутбук, 1 проектор, 1 экран, 1 коммутатор, 1 доска магнитная маркерная. Досмотровый комплект зеркал «Поиск-2У», Комплект сменных щупов «КЩ-3М», Переносной комплект технических средств для обследования автотранспорта «Гастроль П», Портативный ультрафиолетовый осветитель «Дозор-В», Прибор для

		углубленной светооптической проверки документов «Генетика-02.01»; Экран Da-liteModel B 152x203. 7 парт со скамьей, 10 столов компьютерных, 1 стол письменный с тумбой, 20 стульев ИЗО.