ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Директор института
Высшая школа экономики и управления

_____И. П. Савельева
23.04.2018

РАБОЧАЯ ПРОГРАММА
к ОП ВО от 27.06.2018 №084-2449

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 заочная
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.
(ученая степень, ученое звание) _____11.04.2018____ (подпись) Е. А. Степанов

Разработчик программы,
к.экон.н., доц., доцент
(ученая степень, ученое звание, должность) _____11.04.2018____ (подпись) Е. А. Степанов

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
		9
Общая трудоёмкость дисциплины	108	108
Аудиторные занятия	12	12
Лекции (Л)	4	4
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	8	8
Лабораторные работы (ЛР)	0	0
Самостоятельная работа (СРС)	96	96
Изучение государственного стандарта 28147-89	30	30
Изучение государственного стандарта Р34.10-2001	30	30
Изучение государственного стандарта Р34.11-94	36	36
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.	3	1	2	0
2	Криптография. Основные понятия и термины. Алгоритмы симметричного шифрования. Факторы безопасности алгоритмов симметричного шифрования. Примеры алгоритмов симметричного шифрования и их программная реализация.	3	1	2	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.	3	1	2	0

4	Криптографические стандарты. Цифровые сертификаты. Иерархия центров авторизации. Серверные и клиентские сертификаты. Безопасные коммуникации.	3	1	2	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. Правила обеспечения безопасности рабочей станции; Выполнение обновлений операционной системы; Выполнение обновлений прикладных программ; Установка антивирусной программы и регулярное обновление антивирусных баз; Настройка персонального брандмауэра.	1
2	2	Криптография. Криптоанализ. Определения. Термины. Стеганография,примеры использования. Факторы безопасности алгоритмов симметричного шифрования. Абсолютно стойкий шифр. Структура блочного алгоритма симметричного шифрования; Симметричное шифрование блока Алгоритмы DES, AES	1
3	3	Основные требования к алгоритмам асимметричного шифрования (шифрования с открытым ключом). Терминология в алгоритмах асимметричного шифрования. Понятие односторонней функции с секретом. Правила модульной арифметики. Способы использования алгоритмов с открытым ключом (зашифровывание/расшифровывание). Цифровая подпись (прямая, арбитражная)	1
4	4	Цифровые сертификаты Стандарт X.509. Спецификации PKI Иерархия центров авторизации цифровых сертификатов. Серверные и клиентские сертификаты. Безопасные коммуникации на основе SSL.	1

5.2. Практические занятия, семинары

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

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	30
Изучение государственного стандарта Р34.10-2001	http://protect.gost.ru/document.aspx?control=7&id=131131	30
Изучение государственного стандарта Р34.11-94	http://ru.wikipedia.org/wiki/%D0%93%D0%9E%D0%A1%D0%A2_%D0%A0_34.11-94	36

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	Экзамен	1

	информационных технологий и средств обеспечения их функционирования в целях информационного сопровождения профессиональной деятельности		
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	Экзамен	1

7.2. Виды контроля, процедуры проведения, критерии оценивания

Вид контроля	Процедуры проведения и оценивания	Критерии оценивания
Экзамен	ответ на вопросы и проверка хода практического занятия	Отлично: Полный ответ на вопрос и решенные задачи Хорошо: Неполный ответ на вопрос и решенные задачи Удовлетворительно: Решенные задачи без ответа на вопрос Неудовлетворительно: Нерешенные задачи и не верный ответ на вопрос

7.3. Типовые контрольные задания

Вид контроля	Типовые контрольные задания
Экзамен	1. Какие характерные проблемы в обеспечении информационной безопасности данных, хранящихся на персональном компьютере (ПК), появляются при подключении ПК к сети Интернет. 2. Перечислите основные негативные последствия слабой защищенности информационной среды организации. 3. Перечислите виды атак на сетевую рабочую станцию. 4. Какие сервисы безопасности используются при защите рабочей станции. 5. Какие сервисы безопасности используются при защите информации, передающейся по открытым каналам Интернет. 6. Перечислите основные правила обеспечения безопасности рабочей станции. 7. Сформулируйте правило Керкхоффа. 8. Дайте определения терминам: криптография, криптология, криптоанализ, ключ, шифр, зашифрование, расшифрование, дешифрование. 10. Сформулируйте факторы безопасности алгоритмов симметричного шифрования. 11. Каков порядок размера ключа современных криптостойких алгоритмов симметричного шифрования. 12. Сформулируйте основные требования к алгоритмам асимметричного шифрования. 13. Почему в асимметричных криптографических алгоритмах используют два ключа: открытый и закрытый. 14. Дайте определение односторонней функции с секретом. 15. Опишите практическую (комбинированную) реализацию зашифровывания алгоритмом асимметричного шифрования. 16. Опишите практическую (комбинированную) реализацию расшифровывания алгоритмом асимметричного шифрования.

	17. Опишите практическую (комбинированную) реализацию цифровой подписи алгоритмом асимметричного шифрования. 18. Назовите отечественные и зарубежные стандарты алгоритмов асимметричного шифрования. 19. Как используется хэш-функция для безопасного хранения пароля. 20. Назовите характерные области применения программ с открытым исходным кодом: Gpg, Pgp, Openssl, TrueCrypt. 21. Для каких ОС можно использовать библиотеки криптографических функций из Pgp sdk и Openssl. 22. Какую информацию хранят цифровые сертификаты. 23. Какую структуру образуют центры авторизации цифровых сертификатов. 24. Для чего используется серверный сертификат. 25. Для чего используется клиентский сертификат. 26. Опишите алгоритм обеспечения безопасных коммуникаций на основе SSL. ОсновыИБВТамДеле.pdf

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 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.	Электронно-библиотечная система Издательства Лань	Интернет / Авторизованный
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)

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
Практические занятия и семинары	118 (3б)	12 рабочих станций