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: 17.03.2021

И. П. Савельева

РАБОЧАЯ ПРОГРАММА

дисциплины Б.1.51 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: 17.03.2021

Е. А. Степанов

Разработчик программы,
доцент

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Коржуков А. Н.
Пользователь: korzhukovan
Дата подписания: 16.03.2021

А. Н. Коржуков

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)
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.
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;

3. Место дисциплины в структуре ОП ВО

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

Б.1.09 Информатика	Не предусмотрены

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
		10
Общая трудоёмкость дисциплины	108	108
Аудиторные занятия:	60	60
Лекции (Л)	12	12
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	48	48
Лабораторные работы (ЛР)	0	0
Самостоятельная работа (СРС)	48	48
Изучение государственного стандарта Р34.10-2001	16	16
Изучение государственного стандарта Р34.11-94	16	16
Изучение государственного стандарта 28147-89	16	16
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.	16	4	12	0
2	Криптография. Основные понятия и термины. Алгоритмы симметричного шифрования. Факторы безопасности алгоритмов симметричного шифрования. Примеры алгоритмов симметричного шифрования и их программная реализация.	16	4	12	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.	14	2	12	0

4	Криптографические стандарты. Цифровые сертификаты. Иерархия центров авторизации. Серверные и клиентские сертификаты. Безопасные коммуникации.	14	2	12	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.	1
6	3	Способы использования алгоритмов с открытым ключом (зашифровывание/расшифровывание). Цифровая подпись (прямая, арбитражная)	1
7	4	Цифровые сертификаты Стандарт X.509. Спецификации PKI Иерархия центров авторизации цифровых сертификатов	1
8	4	Серверные и клиентские сертификаты. Безопасные ком-муникации на основе SSL.	1

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	6
3,4	1	Использование и защита почтовых протоколов	6
5,6	2	Криптоанализ зашифрованного текста	6
7,8	2	Использование PGP и GPG для обеспечения конфиденциальности электронной почты и шифрования файлов	6
9,10	3	Использование PKI (инфраструктуры открытых ключей) для защиты электронной почты и web-коммуникаций в таможенных органах	6
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.	6
13,14	4	Серверные и клиентские сертификаты. Безопасные коммуникации на базе SSL	6
15,16	4	Цифровые сертификаты Стандарт X.509. Спецификации PKI Иерархия	6

		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 Р34.11-94	http://ru.wikipedia.org/wiki/%D0%93%D0%9E%D0%A1%D0%A2_%D0%A0_34.11-94	16
Изучение государственного стандарта Р34.10-2001	http://protect.gost.ru/document.aspx?control=7&id=131131	16
Изучение государственного стандарта 28147-89	http://protect.gost.ru/document.aspx?control=7&id=139177	16

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

Инновационные формы обучения	Краткое описание и примеры использования в темах и разделах
При оценивании результатов мероприятий используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179).	Оценка результатов обучения и уровня сформированности компетенций проводится в ходе текущей и промежуточной аттестаций с использованием фондов оценочных средств и с применением балльно-рейтинговой системы оценки успеваемости обучающихся. Общее количество баллов при проведении текущего контроля должно быть не менее 60, но не более 100. При неудовлетворительном оценивании одного из показателей компетенции общая оценка также неудовлетворительная.

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	Экзамен	1
Все разделы	ПК-32 владением навыками применения в таможенном деле информационных технологий и средств обеспечения их функционирования в целях информационного сопровождения профессиональной деятельности	текущий	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	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. На экзамене происходит оценивание учебной деятельности обучающихся по дисциплине на основе полученных оценок за контрольно-рейтинговые мероприятия текущего контроля. Студенту необходимо ответить на 20 тестовых вопросов.Время, отведенное на тестирование - 20 минут. При оценивании результатов учебной деятельности обучающегося по дисциплине используется балльно-рейтинговая система оценивания результатов учебной деятельности	Отлично: Величина рейтинга обучающегося по дисциплине 85…100 % Хорошо: Величина рейтинга обучающегося по дисциплине 75…84 % Удовлетворительно: Величина рейтинга обучающегося по дисциплине 60…74 % Неудовлетворительно:

	обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179). Правильный ответ соответствует 0,5 баллам. Максимальное количество баллов – 10. Весовой коэффициент мероприятия – 0,1.	Неудовлетворительно: Величина рейтинга обучающегося по дисциплине 0…59 %
текущий	Проведение контрольных работ. Вопросы представлены на сайте курса эл. ЮУрГУ. При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179). Критерии оценивания : - работа соответствует тематике, полные ответы – 10-9 баллов ; работа соответствует тематике, неполная информация - 1-8 баллов, задача не выполнена – 0 баллов. Весовой коэффициент мероприятия –0,1	Зачтено: рейтинг обучающегося за мероприятие больше или равен 60 %. Не зачтено: рейтинг обучающегося за мероприятие менее 60 %.

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
текущий	

8. Учебно-методическое и информационное обеспечение дисциплины

Печатная учебно-методическая документация

а) основная литература:

Не предусмотрена

б) дополнительная литература:

Не предусмотрена

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-Windows(бессрочно)

2. Microsoft-Office(бессрочно)
3. ООО Альта-софт-Альта-Максимум (версия PRO)(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 ультрофиолетовый 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 ультрофиолетовый 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 ультрофиолетовый 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.