Государственное образовательное автономное учреждение
высшего образования Курской области
«Курская академия государственной и муниципальной службы»
Кафедра философии, социально-правовых и естественнонаучных дисциплин

Утверждаю:
Проректор по учебно-методическому
обеспечению _____ Е.А.Никитина
«31» августа 2022 г.

Рабочая программа дисциплины
«Информационная безопасность в таможенных органах»

Специальность 38.05.02 Таможенное дело
Направленность (профиль) «Таможенная логистика»
Уровень подготовки: специалитет
Форма обучения: очная
Год начала подготовки по УП: 2018

Курск 2022

1. Цели и задачи освоения дисциплины

Цель дисциплины - обучить обучающихся принципам обеспечения информационной безопасности таможенных органов, определить подходы к решению задач обеспечения информационной безопасности компьютерных систем таможенных органов.

Задачи дисциплины – дать основы:

- обеспечения информационной безопасности государства;
- обеспечения информационной безопасности таможенных органов;
- методологии создания систем защиты информации;
- процессов сбора, передачи и накопления информации;
- методов и средств ведения информационных войн;
- оценки защищенности и обеспечения информационной безопасности компьютерных систем таможенных органов.

2. Планируемые результаты обучения, соотнесенные с планируемыми результатами освоения образовательной программы

В результате изучения курса обучающиеся должны:

знать:

– способы сбора, передачи, хранения информации;

– основные понятия и общеметодологические принципы теории информационной безопасности;

– роль информационной безопасности в обеспечении национальной безопасности государства в целом и таможенных органов в частности;

– основные методы нарушения конфиденциальности, целостности и доступности информации;

– основные причины, виды, каналы утечки и искажения информации;

– основные направления обеспечения информационной безопасности объектов информационной сферы таможенных органов.

уметь:

– подбирать и использовать соответствующие правовые, организационно-технические и экономические методы обеспечения информационной безопасности объектов таможенных органов.

владеть:

– навыками анализа информационной инфраструктуры таможенных органов;

– навыками формальной постановки и решения задачи обеспечения информационной безопасности выбранного объекта таможенных органов.

Компетенции обучающегося, формируемые в результате освоения дисциплины «Информационная безопасность в таможенных органах»:

ОПК-1 - способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

ПК-32 - владение навыками применения в таможенном деле информационных технологий и средств обеспечения их функционирования в целях информационного сопровождения профессиональной деятельности;

ПК-34 - способность обеспечивать информацией в сфере таможенного дела государственные органы, организации и отдельных граждан;

ПК-35 - владение навыками использования электронных способов обмена информацией и средств их обеспечения, применяемых таможенными органами.

3. Место дисциплины в структуре образовательной программы

Дисциплина «Информационная безопасность в таможенных органах» относится к дисциплинам по выбору Б1.В ООП. «Информационная безопасность в таможенных

органах» поддерживает межпредметные связи с дисциплинами «Экономическая безопасность», «Информационные таможенные технологии».

4. Объем дисциплины в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу с преподавателем и на самостоятельную работу обучающихся

4.1 Очная форма обучения

Вид работы	Трудоемкость в зач. ед. (часах)	
	3 семестр	Всего
Общая трудоемкость	2 (72)	2 (72)
Контактная работа	0,78 (28)	0,78 (28)
лекции практические (семинарские) занятия	0,39 (14) 0,39 (14)	0,39 (14) 0,39 (14)
Самостоятельная работа	1,22 (44)	1,22 (44)
Контроль	-	-
Контрольные формы	**Зачет**	**Зачет**

5. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических или астрономических часов и видов учебных занятий

5.1. Очная форма обучения

№	Наименование раздела (темы)	Всего часов в трудоем-кости	В том числе контактная работа				Сам. работа (инд.) работа
			Всего	Лекций	Практ. занятий	Лабор. занятий	
1	Информационная безопасность в системе национальной безопасности Российской Федерации.	8	2	2	-	-	6
2	Информационная безопасность таможенных органов в структуре национальной безопасности Российской Федерации.	8	2	-	2	-	6
3	Виды угроз информационной безопасности Таможенным органам.	6	2	2	-	-	4
4	Источники угроз информационной безопасности таможенных органов.	6	2	-	2	-	4
5	Информационная безопасность и информационное противоборство.	8	4	2	2	-	4

6	Обеспечение информационной безопасности объектов информатизационной сферы таможенных органов.	6	2	2	-	-	4
7	Общие методы обеспечения информационной безопасности таможенных органов	8	4	2	2	-	4
8	Основы комплексного обеспечения информационной безопасности таможенных органов.	8	2	2	-	-	6
9	Методы и средства обеспечения информационной безопасности компьютерных систем.	14	8	2	6	-	6
	Контроль	-	-	-	-	-	-
	Всего	72	28	14	14	-	44

5.2 Содержание семинарских (практических) занятий

Семинарское занятие № 1. «Информационная безопасность в системе национальной безопасности Российской Федерации»

1. Чем отличается стеганография от криптографии?
2. Какие основные направления стеганографии?
3. В чем различия в работе с программами Image Hide и Steganography?

Семинарское занятие № 2. «Информационная безопасность таможенных органов в структуре национальной безопасности»

1. Назовите факторы, определяющие сложность пароля.
2. Какие пароли являются не криптостойкими?
3. Назовите требования для формирования криптостойкого пароля?

Семинарское занятие № 3. «Виды угроз информационной безопасности Таможенным органам. Создание защищенных PDF файлов»

1. Для чего предназначен формат Portable Document Format (PDF)?
2. Какие ограничения можно установить при создании защищенного PDF файла?
3. От каких угроз информационной безопасности защищают ограничения PDF файлов?

Семинарское занятие № 4. «Источники угроз информационной безопасности таможенных органов. Создание зашифрованных файлов»

1. Укажите особенности работы в программах Protectorion ToGo и Simple File Encryptor.
2. Что такое алгоритмы шифрования?
3. От каких угроз информационной безопасности защищает шифрование файлов?

Семинарское занятие № 5. «Информационная безопасность и информационное противоборство. Восстановление удаленных файлов»

1. Укажите особенности работы в программах Recuva, Handy Recovery и Pandora Recovery.
2. Как работает механизм восстановления данных?

3. Какие угрозы информационной безопасности предотвращает восстановление файлов?

Семинарское занятие № 6. «Обеспечение информационной безопасности объектов информатизационной сферы таможенных органов»

1. Укажите особенности работы в программе Dr.WebLiveUSB.
2. Какие программные приложения входят в состав Dr.WebLiveUSB?
3. Какие угрозы информационной безопасности предотвращает Dr.WebLiveUSB?

Семинарское занятие № 7. «Общие методы обеспечения информационной безопасности таможенных органов»

1. Укажите основные правовые акты в области информационной безопасности.

Семинарское занятие № 8. «Основы комплексного обеспечения информационной безопасности таможенных органов»

1. Концепция ИБ таможенных органов.
2. Комплексная защита информации.
3. Этапы развертывания КСЗИ.
4. Перечислите основные характеристики КСЗИ.
5. Выявите какие элементы КСЗИ необходимы для разных уровней организации защиты Таможни, ТП, РТУ.

Семинарское занятие № 9. «Методы и средства обеспечения информационной безопасности компьютерных систем»

1. Ведомственная сеть ФТС и способы организации защиты информации в ней.
2. Защита БД ФТС
3. Подходы к защите информации в компьютерных системах.
4. Перечислите основные угрозы ИБ ФТС в рамках реализации ведомственной сети.
5. Назовите классификацию компьютерных вирусов.
6. Аппаратно-программные системы защиты информации.
7. Файервол это?

6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Развитие самостоятельности как качества личности является одной из важнейших задач обучения. Термин «самостоятельность» обозначает такое действие человека, которое он совершает без непосредственной или опосредованной помощи другого человека, руководствуясь лишь собственными представлениями о порядке и правильности выполняемых операций.

Самостоятельная работа обучающихся по усвоению учебного материала может выполняться в читальном зале библиотеки, учебных кабинетах (лабораториях), компьютерных классах, дома. Обучающийся подбирает научную и специальную монографическую и периодическую литературу в соответствии с рекомендациями преподавателя или самостоятельно.

При организации самостоятельной работы с использованием технических средств, обеспечивающих доступ к информации (компьютерных баз данных, систем автоматизированного проектирования и т.п.), должно быть предусмотрено и получение необходимой консультации или помощи со стороны преподавателей.

Самостоятельная работа требует наличия информационно-предметного обеспечения: учебников, учебных и методических пособий, конспектов лекций. Методические материалы должны обеспечивать возможность самоконтроля обучающихся по блоку учебного материала или предмета в целом.

Творческий подход преподавателя к осмыслению (интериоризации) приведенной информации поможет созданию оптимальных условий для использования понятия «самостоятельность» не только как формы организации учебного процесса, но и как одного из недостаточно раскрытых резервов категории «познавательная деятельность» в обучении.

Самостоятельная работа обучающихся по дисциплине «Информационная безопасность в таможенных органах» включает в себя:

- текущую работу над учебным материалом, изложенным в учебниках, учебных пособиях и дополнительной литературе по заданию преподавателя;
- изучение и дополнение своих лекционных записей с использованием основной и дополнительной литературы;
- подготовку научных сообщений и докладов на семинарские занятия, коллективные презентации, научные семинары, лекции-конференции.
- выполнение письменных заданий и тестов,
- самоконтроль приобретенных знаний;
- подготовку к зачету.

Важнейшими принципами самостоятельной работы являются:

- регулярность: занимайтесь не от случая к случаю, а регулярно;
- целенаправленность: прежде чем начать работать с научным текстом (учебником, монографией, статьей из журнала, сайтом из Интернета и др.), решите, что Вы хотите узнать, на какие вопросы получить ответы;
- последовательность: не стремитесь забежать вперёд, узнать всё сразу, вместо быстрого, но поверхностного усвоения содержания дисциплины практикуйте постепенное и последовательное движение в соответствии с программой курса – так вы сделаете свои знания более прочными;
- практичность: старайтесь распознать практическое значение даже самых абстрактных, казалось бы, оторванных от реальной жизни, идей и теорий, методов и концепций, оценить сквозь их призму собственную профессиональную деятельность, как прошлую и нынешнюю, так и будущую, применить получаемые на занятиях знания для понимания прошлого, настоящего и будущего нашей страны и всего человечества;
- критицизм: не принимайте всё, что услышите и прочитаете, за «чистую монету»; следуя советам древних мыслителей, сомневайтесь во всём, дерзайте вопрошать и критиковать авторитеты – так вы не только разовьете навыки самостоятельного мышления, но и сделаете полученные знания более прочными и упорядоченными;
- коллегиальность: обсуждайте прочитанное в книгах и газетах, услышанное и увиденное по телевизору и на занятиях в кругу своих товарищей - ведь именно в споре рождается истина.

Задачи для самостоятельной работы

Цифровая подпись подтверждает ваше авторство и обеспечивает целостность письма или файла. Для цифровой подписи вы используете свой закрытый ключ, а проверить авторство документа может кто угодно с помощью вашего открытого ключа. Степень защиты цифровой подписи от подделки такая же высокая, как степень стойкости при шифровании с помощью PGP/GnuPG.

Чтобы подписать содержимое буфера обмена:

1. Выделите текст (например, в редакторе почтового клиента или в текстовом редакторе) и скопируйте его в буфер ([Ctrl]+[C]).
2. Щелкните по изображению замочка (GPGTray) в правом нижнем углу экрана и выберите в меню Подписать буфер (откр. текст).
3. Программа предложит вам все доступные закрытые ключи. Выберите нужный ключ, нажмите OK. Введите пароль, нажмите Enter. Теперь в буфере обмена находится уже не оригинальный, а зашифрованный текст. Можете вставить его в редактор своей почтовой программы командами меню или сочетанием клавиш [Ctrl]+[V].
4. Чтобы проверить подпись, нужно выбрать в меню PGPtray пункт Расшифровать/Проверить буфер. Для окна: Активное окно – Расшифровать/Проверить/Импорт. Вот что должно получиться в результате:

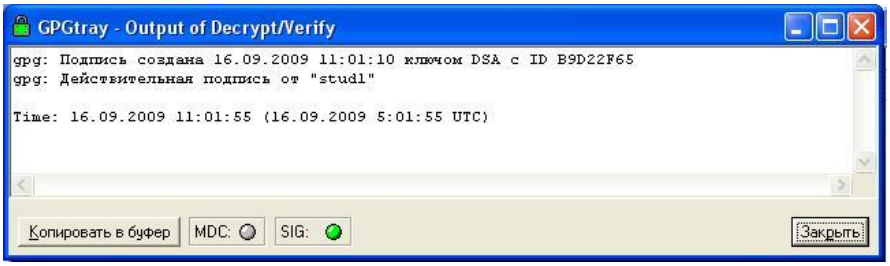

Рис. 29 Окно цифровой подписи

Шифрование и электронная подпись могут с успехом применяться вместе. Подпись удостоверяет личность, шифрование защищает письмо от чужих глаз. Сделать это можно, выбирая не Зашифровать или Подписать по отдельности, а Зашифровать и подписать. Такой ход мешает злоумышленнику просто изъять из письма цифровую подпись.

Задание для самостоятельного выполнения

Произведите шифрование и электронную подпись документа в формате .doc, используя следующие программы:

1. **GFileProtect 1.2** Программа предназначена для защиты личной информации путем ее шифрования. В качестве алгоритма шифрования используется американский стандарт Advanced Encryption Standard (AES). Шифровать можно любе файлы не зависимо от формата данных.
2. **Locker full set 1.1** Многоуровневая защита ваших данных. Ключ для шифрования файлов создается каждый раз на основе пароля, введенного вами, что исключает взлом защиты путем получения ключа и вам не нужно заботиться о его хранении. Если вы при шифровании используете USB диск (флешку), ваши файлы никто не сможет расшифровать даже зная пароль, пока не будет вставлен именно ваш USB диск. Программа ничего не создает на вашем USB диске, а только идентифицирует его.
3. **Locker (шифрование файлов) 1.1** Шифрование файлов – наиболее надежная защита ваших данных. Программа Locker (шифрование файлов) позволяет шифровать любые файлы любого размера и в любом количестве с высокой скоростью. Вы можете также использовать USB-защиту при шифровании файлов, в этом случае никто не сможет их расшифровать даже зная пароль, пока не будет вставлен именно ваш USB диск (флешка).
4. **Secure Disk 2.1** Мощный криптографический продукт нового поколения с предзагрузочной аутентификацией защищает 100% вашего жесткого диска, включая операционную систему.

Программа Secure Disk позволяет шифровать информацию на вашем компьютере, полностью шифруя содержимое ваших дисков на уровне физических секторов.

Немаловажным свойством приложения Secure Disk является то, что оно работает не только с жестким диском компьютера, но и с flash-носителями. Таким образом, вам не нужно бояться того, что в случае потери flash-носителя, им сможет кто-нибудь воспользоваться в корыстных целях.

Основной и единственной функцией программы Secure Disk является шифрование информации, расположенной на жестком диске и на флеш-носителях.

5. **RSACryptoSystem 2.0** Программа идеально подходит для защиты любой конфеденциальной информации как на локальном компьютере, так и при обмене информацией в сетях любого типа (включая ЛВС и Интернет).В программе есть возможность шифрования файлов как по паролю, так и с использованием ключевых файлов. Программа проста в освоении и имеет русскоязычный интерфейс, а также подробнейшую справку на русском языке.

Вопросы для самостоятельного изучения

1. Чем отличается стеганография от криптографии?
2. Какие основные направления стеганографии?
3. В чем различия в работе с программами Image Hide и Steganography?
4. Назовите факторы, определяющие сложность пароля.

5. Какие пароли являются не криптостойкими?
6. Назовите требования для формирования криптостойкого пароля?
7. Для чего предназначен формат Portable Document Format (PDF)?
8. Какие ограничения можно установить при создании защищенного PDF файла?
9. От каких угроз информационной безопасности защищают ограничения PDF файлов?
10. Укажите особенности работы в программах Protectorion ToGo и Simple File Encryptor.
11. Что такое алгоритмы шифрования?
12. От каких угроз информационной безопасности защищает шифрование файлов?

Примерная тематика рефератов:

1. Средства и механизмы обеспечения аудита и методы анализа данных аудита.
2. Анализ безопасности DNS технологии.
3. Методы и средства контроля и сохранения целостности сетевого трафика.
4. Доступ на основе одноранговых паролей – достоинства и недостатки, методы и средства взлома.
5. Комплексный подход к построению систем антивирусной защиты.
6. Средства анализа защищенности компьютерной системы.
7. Защита информации в системах электронной почты.
8. Системы обнаружения сетевых атак.
9. Виды и средства атак на локальный компьютер.
10. Виды и средства атак на удаленный компьютер в сети.
11. Особенности и средства защиты информации в беспроводных сетях.
12. Виртуальные приватные сети (VPN). Сравнительный анализ средств построения.
13. Анализ возможности обеспечения безопасности в ОС Windows.
14. Сетевые атаки. Особенности, методы и средства защиты.
15. Методы и средства поиска программ-закладок и недокументированных функций в программном обеспечении.
16. Методы и средства считывания удаленных данных и данных с поврежденных магнитных носителей информации.
17. Методы и средства выявления сканирования портов.
18. Методы «социальной инженерии».
19. Политика безопасности организации – структура и особенности.
20. Анализ рисков информационной безопасности в компьютерных системах.
21. Управление рисками информационной безопасности в компьютерных системах.
22. Разработка рекомендаций работы с персоналом предприятия по обеспечению информационной безопасности.
23. Специфика проведения расследования инцидентов в сфере информационной безопасности.
24. Аварийный план действий в случае совершения атаки – структура и средства поддержки.
25. Сетевые вирусы. Особенности. Средства и способы удаления и предупреждения заражения.
26. Защита речевой информации при ее передаче по каналам связи.
27. Защита акустической информации, циркулирующей в защищаемых помещениях.
28. Правовое обеспечение информационной безопасности.
29. Методы и средства защиты интеллектуальной собственности.
30. Идентификация пользователей и установление их подлинности при доступе к компьютерным ресурсам.
31. Организация защищенного документооборота.
32. Анализ и оценка угроз информационной безопасности объекта.
33. Оценка ущерба вследствие противоправного раскрытия информации

ограниченного доступа.
34. Средства и методы физической защиты объектов.
35. Организация пропускного и внутриобъектового режима.
36. Организационные методы обеспечения информационной безопасности.
37. Защита информации при авариях и экстремальных ситуациях.
38. Обеспечение информационной безопасности учреждения при осуществлении международного научно-технического и экономического сотрудничества
39. Организационные и технические мероприятия, используемые для противодействия технической разведке.
40. Методы и средства защиты режимных объектов от утечки конфиденциальной информации по каналам электромагнитных излучений и наводок.
41. Угрозы информационно-программному обеспечению вычислительных систем и их классификация.
42. Многоуровневая структура системы защиты на основе программно-аппаратных средств вычислительной системы.
43. Парольное разграничение доступа и комбинированные методы.
44. Защита программных средств от несанкционированного копирования, исследования и модификации.
45. Технология гарантированного восстановление вычислительной системы после заражения компьютерными вирусами.
46. Проблемы ключей системы шифрования.
47. Установление подлинности, электронная цифровая подпись.
48. Технология восстановления дисковой и оперативной памяти.
49. Особенности защиты информации в базах данных.
50. Защита программ от изменения и контроль целостности.
51. Использование межсетевых экранов (брандмауэров) для защиты информации в локальных вычислительных сетях.
52. Защита документа в Microsoft Office.

7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

7.1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Наименование разделов, тем	Код формируемой компетенции	Образовательные технологии (очная/заочная формы)	Этап освоения компетенции
Информационная безопасность в системе национальной безопасности Российской Федерации.	ОПК-1 ПК-32 ПК-34	Лекция, самостоятельная работа	Начальный Начальный Начальный
Информационная безопасность таможенных органов в структуре национальной безопасности Российской Федерации.	ОПК-1 ПК-32 ПК-34	Практическое занятие, самостоятельная работа	Начальный Начальный Начальный
Виды угроз информационной безопасности Таможенным органам.	ОПК-1 ПК-32 ПК-34	Лекция, самостоятельная работа	Начальный Начальный Начальный

Источники угроз информационной безопасности таможенных органов.	ОПК-1 ПК-32 ПК-34	Практическое занятие, самостоятельная работа	Начальный Начальный Начальный
Информационная безопасность и информационное противоборство.	ОПК-1 ПК-32 ПК-34	Лекция, практическое занятие, самостоятельная работа	Начальный Начальный Начальный
Обеспечение информационной безопасности объектов информатизационной сферы таможенных органов.	ОПК-1 ПК-32 ПК-34	Лекция, самостоятельная работа	Начальный Начальный Начальный
Общие методы обеспечения информационной безопасности таможенных органов	ПК-32 ПК-34 ПК-35	Лекция, практическое занятие, самостоятельная работа	Начальный Начальный Начальный
Основы комплексного обеспечения информационной безопасности таможенных органов.	ПК-32 ПК-34 ПК-35	Практическое занятие, самостоятельная работа	Начальный Начальный Начальный
Методы и средства обеспечения информационной безопасности компьютерных систем	ОПК-1 ПК-32 ПК-34	Лекция, практическое занятие, самостоятельная работа	Начальный Начальный Начальный

7.2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования

№ п/п	Код компетенции	Показатели и критерии оценивания на различных этапах формирования			Оценочные средства
		Пороговый (удовлетворительно)	**Продвинутый (хорошо)**	**Высокий (отлично)**	
1.	**ОПК-1**	Знать: понятие информации, свойства информации, виды информации; понятие алгоритма, виды алгоритмов. Уметь: использовать знания по теории информации при решении задач; использовать знания по	Знать: основные области применения ЭВМ; основные принципы устройства ЭВМ. Уметь: применять знания архитектуры ЭВМ в профессиональной деятельности; организовывать	Знать: виды системного и прикладного программного обеспечения ЭМВ; основные методы поиска в Интернет; технологию обработки графической информации; технологию обработки текстовой информации; технологию	Вопросы к зачету, тестовые задания, отчеты по практическим работам

		алгоритмизации в профессиональ-ной деятельности. Владеть: основами автоматизации работы с информацией.	поиск и безопасную работу в Интернет. Владеть: способами алгоритмизации информации.	обработки числовой информации. Уметь: использовать технологию обработки графической информации; использовать технологию обработки текстовой информации; использовать технологию обработки числовой информации. Владеть: способами применения ЭВМ в различных областях; различными способами классификации программного обеспечения ЭВМ; основными способами безопасной работы в сети Интернет; технологиями обработки текстовой, числовой и графической информации.	
2.	**ПК-32**	Знать: понятие информации, свойства информации, виды информации. Уметь: использовать знания по теории информации при решении задач; использовать знания по	Знать: понятие алгоритма, виды алгоритмов. Уметь: применять знания архитектуры ЭВМ в профессиональ-ной деятельности; организовывать поиск и	Знать: основные принципы устройства ЭВМ; виды системного и прикладного программного обеспечения ЭМВ; основные методы поиска в Интернет; технологию обработки графической информации;	Вопросы к зачету, тестовые задания, отчеты по практиче-ским работам

		алгоритмизации в профессиональ-ной деятельности. Владеть: основами автоматизации работы с информацией.	безопасную работу в Интернет; использовать технологию обработки графической информации. Владеть: способами алгоритмизации информации.	технологию обработки текстовой информации; технологию обработки числовой информации. Уметь: использовать технологию обработки текстовой информации; использовать технологию обработки числовой информации. Владеть: различными способами классификации программного обеспечения ЭВМ; основными способами безопасной работы в сети Интернет; технологиями обработки текстовой, числовой и графической информации.	
3.	**ПК-34**	Знать: понятие информации, свойства информации, виды информации; понятие алгоритма, виды алгоритмов. Уметь: использовать знания по теории информации при решении задач; использовать знания по алгоритмизации в	Знать: основные области применения ЭВМ; основные принципы устройства ЭВМ. Уметь: применять знания архитектуры ЭВМ в профессиональ-ной деятельности; организовывать поиск и	Знать: виды системного и прикладного программного обеспечения ЭМВ; основные методы поиска в Интернет; технологию обработки графической информации; технологию обработки текстовой информации; технологию обработки	Вопросы к зачету, тестовые задания, отчеты по практичес-ким работам

		профессиональ-ной деятельности. Владеть: основами автоматизации работы с информацией.	безопасную работу в Интернет. Владеть: способами алгоритмизации информации.	числовой информации. Уметь: использовать технологию обработки графической информации; использовать технологию обработки текстовой информации; использовать технологию обработки числовой информации. Владеть: способами применения ЭВМ в различных областях; различными способами классификации программного обеспечения ЭВМ; основными способами безопасной работы в сети Интернет; технологиями обработки текстовой, числовой и графической информации.	
4.	**ПК-35**	Знать: понятие информации, свойства информации, виды информации. Уметь: использовать знания по теории информации при решении задач; использовать знания по алгоритмизации в	Знать: понятие алгоритма, виды алгоритмов. Уметь: применять знания архитектуры ЭВМ в профессиональ-ной деятельности; организовывать поиск и безопасную	Знать: основные принципы устройства ЭВМ; виды системного и прикладного программного обеспечения ЭМВ; основные методы поиска в Интернет; технологию обработки графической информации; технологию	Вопросы к зачету, тестовые задания, отчеты по практичес-ким работам

		профессиональ-ной деятельности. Владеть: основами автоматизации работы с информацией.	работу в Интернет; использовать технологию обработки графической информации. Владеть: способами алгоритмизации информации.	обработки текстовой информации; технологию обработки числовой информации. Уметь: использовать технологию обработки текстовой информации; использовать технологию обработки числовой информации. Владеть: различными способами классификации программного обеспечения ЭВМ; основными способами безопасной работы в сети Интернет.	

7.3 Шкала оценивания сформированности компетенций

Шкала оценивания	Критерии		Результат
	Устный ответ	Тестирование	
«отлично»	– полно раскрыто содержание материала; – материал изложен грамотно, в определенной логической последовательности; – продемонстрировано системное и глубокое знание программного материала; – точно используется терминология; – показано умение иллюстрировать теоретические положения конкретными примерами, применять их в новой ситуации; – продемонстрировано усвоение ранее изученных сопутствующих вопросов, сформированность и устойчивость компетенций, умений и навыков; – ответ прозвучал самостоятельно, без наводящих вопросов;	от 100 до 35% правильных ответов	**зачтено**

	– продемонстрирована способность творчески применять знание теории к решению профессиональных задач; – продемонстрировано знание современной учебной и научной литературы; – допущены одна – две неточности при освещении второстепенных вопросов, которые исправляются по замечанию.		
«хорошо»	– вопросы излагаются систематизировано и последовательно; – продемонстрировано умение анализировать материал, однако не все выводы носят аргументированный и доказательный характер; – продемонстрировано усвоение основной литературы. – ответ удовлетворяет в основном требованиям на оценку «5», но при этом имеет один из недостатков: в изложении допущены небольшие пробелы, не исказившие содержание ответа; допущены один – два недочета при освещении основного содержания ответа, исправленные по замечанию преподавателя; допущены ошибка или более двух недочетов при освещении второстепенных вопросов, которые легко исправляются по замечанию преподавателя.	от 75% до 50 % правильных ответов	**зачтено**
«удовлетворительно»	– неполно или непоследовательно раскрыто содержание материала, но показано общее понимание вопроса и продемонстрированы умения, достаточные для дальнейшего усвоения материала; – усвоены основные категории по рассматриваемому и дополнительным вопросам; – имелись затруднения или допущены ошибки в определении понятий, использовании терминологии, исправленные после нескольких наводящих вопросов; – при неполном знании	от 50% до 35% правильных ответов	**зачтено**

	теоретического материала выявлена недостаточная сформированность компетенций, умений и навыков, обучающийся не может применить теорию в новой ситуации; – продемонстрировано усвоение основной литературы.		
«неудовлетворительно»	- не раскрыто основное содержание учебного материала; – обнаружено незнание или непонимание большей или наиболее важной части учебного материала; – допущены ошибки в определении понятий, при использовании терминологии, которые не исправлены после нескольких наводящих вопросов - не сформированы компетенции, умения и навыки, - отказ от ответа или отсутствие ответа	менее 35% правильных ответов	**не зачтено**

7.4 Типовые контрольные задания и (или) иные материалы, применяемые для оценки знаний, умений и навыков и/или опыта деятельности, характеризующие этапы формирования компетенций в процессе освоения образовательной программы

Вопросы к зачету

1. Понятие национальной безопасности.
2. Виды безопасности и сферы жизнедеятельности личности, общества и государства.
3. Определение информационной безопасности
4. Место информационной безопасности в системе национальной безопасности
5. Интересы личности в информационной сфере
6. Интересы общества в информационной сфере
7. Интересы государства в информационной сфере
8. Угрозы информационному обеспечению государственной политики Российской Федерации
9. Виды угроз информационной безопасности
10. Внешние источники угроз информационной безопасности
11. Внутренние источники угроз информационной безопасности государства.
12. Информационное оружие, его классификация и возможности.
13. Доктрина информационной войны
14. Методы и средства ведения информационной войны
15. Понятие информационного противоборства
16. Причины искажения информации,
17. Виды искажения информации
18. Каналы утечки информации
19. Естественные и искусственные каналы утечки информации
20. Правовые, организационно-технические и экономические методы обеспечения информационной безопасности.
21. Критерии и классы защищенности средств ВТ
22. Компьютерная система как объект информационной безопасности.
23. Информационные процессы как объект информационной безопасности
24. Влияние человеческого фактора на обеспечение информационной безопасности

25. Программно-аппаратные средства обеспечения информационной безопасности.
26. Классификация программно-аппаратных средств обеспечения информационной безопасности
27. Защита от несанкционированного доступа
28. Антивирусная защита
29. Межсетевые экраны
30. VPN-технологии
31. Криптографические методы защиты информации

Тестовые задания:

1. Государственная тайна - это принадлежащие государству (государственному учреждению) сведения о его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности государства. В соответствии с законом РФ «О государственной тайне» таким сведениям может быть присвоен соответствующий гриф секретности:

1) «совершенно секретно»
2) «совсем секретно»
3) «секретно»
4) «не секретно»
5) «особой важности»

2. С любым объектом информационной безопасности естественным образом связано существование той или иной угрозы, под которой понимается

1) совокупность условий и факторов, возникающих в процессе взаимодействия данного объекта с другими объектами или составляющих его компонентов между собой и способных оказывать на него негативное воздействие.
2) совокупность условий и факторов, возникающих в процессе взаимодействия данного объекта с другими объектами или составляющих его компонентов между собой и способных оказывать на него благоприятное воздействие.
3) негативное воздействие на объект информационной безопасности, возникающее в процессе взаимодействия данного объекта с другими объектами или составляющих его компонентов между собой

3. Сопоставьте определение и понятие

1) взаимосвязанная совокупность средств, методов и персонала, обеспечивающих сбор, хранение, обработку, передачу и отображение информации в интересах достижения поставленной цели	1) Информационная технология (ИТ)
2) совокупность средств и методов сбора, обработки, передачи данных (первичной информации) для получения информации нового качества (информационного продукта) о состоянии объекта, процесса или явления	2) Информационная система (ИС)

4. Информационное оружие от обычных средств поражения отличает:

1) универсальность - возможность многовариантного использования его как военными, так и гражданскими структурами нападающей стороны против военных и гражданских объектов страны поражения
2) существенность - создание национальных и международных информационных ресурсов
3) скрытность - способность достигать цели без видимой подготовки и объявления войны
4) масштабность - возможность наносить невосполнимый ущерб, невзирая на национальные границы и суверенитеты

5. В отсутствие строгого определения информация интуитивно рассматривается в широком смысле как:

1) любые данные или сведения об объектах или явлениях окружающей среды, их параметрах, свойствах и состоянии

2) некое отражение реального мира с помощью различных сведений и сообщений

6. Сопоставьте определение и понятие

1) интегральная характеристика, выражающая свойства защищённости компьютерной системы в терминах, представляющих эту систему.	1) При этом под концепцией информационной безопасности понимается
2) официально принятая система взглядов на проблему информационной безопасности на уровне государства, отрасли или отдельной организации	2) Политика безопасности - это

7. Соотнесите наиболее важные свойства информации и определения

1) это свойство, указывающее на необходимость введения ограничений доступа к данной информации для определенного круга лиц	1) Целостность
2) это свойство, характеризующее способность обеспечивать своевременный и беспрепятственный доступ пользователей к необходимой информации	2) Доступность
3) это свойство, заключающееся в существовании информации в неискаженном виде по отношению к некоторому фиксированному состоянию	3) Конфиденциальность

8. Классификация угроз информационной безопасности компьютерных систем может быть проведена по ряду базовых признаков. Сопоставьте признак и классификацию

1) Природная среда. Человек. Санкционированные программно-аппаратные средства. Несанкционированные программно-аппаратные средства.	1) По степени преднамеренности проявления
2) Естественные угрозы. Искусственные угрозы	2) По непосредственному источнику угроз
3) Вне контролируемой зоны, территории (помещения). В пределах контролируемой зоны	3) По положению источника угроз
4) Случайные угрозы. Преднамеренные угрозы.	4) По природе возникновения

9. В информационных процессах, протекающих в обществе, используется, с одной стороны, массовая информация, предназначенная для неограниченного круга лиц, а с другой стороны - конфиденциальная информация, доступ к которой ограничивается либо ее собственником, либо соответствующим законодательством. Конфиденциальная информация может содержать ... или ... тайну.

1) Секретную
2) Государственную
3) Совершенно секретную
4) Коммерческую

10. Сопоставьте определение и принципы информационной безопасности

1) Суть этого принципа состоит в том, что защита информации не должна обеспечиваться только за счёт секретности структурной и функциональной организации системы защиты.	1) Гибкость системы защиты
2) Предполагает необходимость учёта всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов	2) Принцип комплексности
3) Часто приходится создавать системы защиты в условиях большой неопределённости. Принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечить	3) Принцип системности

как чрезмерный, так и недостаточный уровень зашиты. Естественно, для обеспечения возможности коррекции этого уровня средства защиты должны обладать определённой гибкостью.	
4) Согласование разнородных средств при построении целостной системы защиты, перекрывающей все существующие, а также возможные каналы реализации угроз и не содержащей слабых мест на стыках отдельных её компонентов	4) Принцип простоты применения средств защиты
5) Предполагающий принятие соответствующих мер на всех этапах жизненного цикла КС (начиная с самых ранних стадий проектирования, а не только на этапе её эксплуатации)	5) Принцип непрерывности защиты
6) Механизмы защиты должны быть интуитивно понятны и просты в использовании. Защита будет тем эффективнее, чем легче пользователю с ней работать.	6) Открытость алгоритмов и механизмов защиты

11. Объектом информационной безопасности выступает:

1) организация
2) секретность
3) методы и средства защиты информации
4) информация
5) сотрудники

12. Защитить информацию - это значит _____.

13. Противодействие многочисленным угрозам информационной безопасности КС предусматривает комплексное использование различных способов и мероприятий организационного, правового, инженерно-технического, программно-аппаратного, криптографического характера и др. Сопоставьте определение и понятие

1) Является многоаспектным понятием, включающим как международные, так и национальные правовые нормы	1) Инженерно-техническая защита информации
2) Суть защиты заключается в приведении (преобразовании) информации к неявному виду с помощью специальных алгоритмов либо аппаратных средств и соответствующих кодовых ключей.	2) Программно-аппаратная защита информации
3) Регламентация производственной деятельности и взаимоотношений исполнителей, осуществляемая на нормативно-правовой основе таким образом, чтобы сделать невозможным или существенно затруднить разглашение, утечку и несанкционированный доступ к конфиденциальной информации за счёт проведения соответствующих организационных мероприятий	3) Криптографическая защита информации
4) Включает в себя физико-технические, аппаратные, технологические, программные, криптографические и другие средства. Создает физически замкнутую среду вокруг элементов защиты, создавая тем самым определённое препятствие для традиционного шпионажа и диверсий.	4) Правовая защита информации
5) Непосредственно применяется в компьютерах и компьютерных сетях, содержат различные встраиваемые в КС электронные, электромеханические устройства. Специальные пакеты программ или отдельные программы реализуют такие функции защиты, как разграничение и контроль доступа к ресурсам, регистрация и анализ	5) Организационная защита информации

протекающих процессов, событий, пользователей, предотвращение возможных разрушительных воздействий на ресурсы, идентификация и аутентификация пользователей и процессов и др.	

14. Документированная информация – это _____.

15. Сопоставьте определение и понятие

1) проверка подлинности идентификации пользователя, процесса, устройства или другого компонента системы (обычно осуществляется перед разрешением доступа); а также проверка целостности и авторства данных при их хранении или передаче для предотвращения несанкционированной модификации.	1) Идентификация - это
2) предоставление субъекту прав на доступ к объекту.	2) Аутентификация - это
3) процесс распознавания элемента системы, обычно с помощью заранее определенного идентификатора или другой уникальной информации; каждый субъект или объект системы должен быть однозначно идентифицируем.	3) Авторизация - это
4) ограничение возможностей использования ресурсов системы программами, процессами или другими системами (для сети) в соответствии с правилами разграничения доступа.	4) Контроль доступа - это

16. Персональные данные – это _____.

17. В методологии анализа информационной безопасности обычно выделяют следующие основные понятия:

1) информационные технологии
2) доктрина информационной безопасности Российской Федерации
3) существующие и потенциально возможные угрозы данному объекту
4) обеспечение информационной безопасности объекта от проявления угроз
5) объект информационной безопасности

18. Что лучше всего описывает цель расчета ALE?

1) Количественно оценить уровень безопасности среды
2) Оценить возможные потери для каждой контрмеры
3) Количественно оценить затраты / выгоды
4) Оценить потенциальные потери от угрозы в год

19. Что является определением воздействия (exposure) на безопасность?

1) Нечто, приводящее к ущербу от угрозы
2) Любая потенциальная опасность для информации или систем
3) Любой недостаток или отсутствие информационной безопасности
4) Потенциальные потери от угрозы

20. Что такое политики безопасности?

1) Пошаговые инструкции по выполнению задач безопасности
2) Общие руководящие требования по достижению определенного уровня безопасности
3) Широкие, высокоуровневые заявления руководства
4) Детализированные документы по обработке инцидентов безопасности

Творческие кейс задания

Задание 1.

С помощью встроенных возможностей операционной системы, проанализируйте загруженность процессора и определите подозрительные процессы. Используйте антивирусную программу для поиска зараженных файлов, составьте перечень работ на рабочем месте, необходимых для организации процесса по определению защищенности информации на рабочем месте служащего.

Задание 2.

Выявите возможные угрозы и определите возможную модель потенциального злоумышленника в рамках таможни или таможенного поста. Определите комплекс мероприятий по устранению уязвимостей.

7.5 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Текущий контроль представляет собой проверку усвоения учебного материала теоретического и практического характера, регулярно осуществляемую на протяжении семестра.

К достоинствам данного типа относится его систематичность, непосредственно коррелирующаяся с требованием постоянного и непрерывного мониторинга качества обучения, а также возможность балльно-рейтинговой оценки успеваемости обучающихся.

Недостатком является фрагментарность и локальность проверки. Компетенцию целиком, а не отдельные ее элементы (знания, умения, навыки) при подобном контроле проверить невозможно.

К основным формам текущего контроля (текущей аттестации) можно отнести устный опрос, письменные задания, лабораторные работы, контрольные работы.

Промежуточная аттестация, как правило, осуществляется в конце семестра и может завершать изучение, как отдельной дисциплины, так и ее раздела (разделов) /модуля (модулей). Промежуточная аттестация помогает оценить более крупные совокупности знаний и умений, в некоторых случаях – даже формирование определенных профессиональных компетенций.

Достоинства: помогает оценить более крупные совокупности знаний и умений, в некоторых случаях – даже формирование определенных профессиональных компетенций.

Основные формы: зачет.

Текущий контроль и промежуточная аттестация традиционно служат основным средством обеспечения в учебном процессе «обратной связи» между преподавателем и обучающимся, необходимой для стимулирования работы обучающихся и совершенствования методики преподавания учебных дисциплин.

Оценивание знаний, умений, навыков и (или) опыта деятельности должно носить комплексный, системный характер – с учетом как места дисциплины в структуре образовательной программы, так и содержательных и смысловых внутренних связей. Связи формируемых компетенций с модулями, разделами (темами) дисциплины обеспечивают возможность реализации для текущего контроля, промежуточной аттестации по дисциплине и итогового контроля наиболее подходящих оценочных средств.

В качестве методических материалов, определяющих процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в академии используются:

- Положение о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся по программам бакалавриата, программам специалитета, программам магистратуры Академии госслужбы, утвержденное ректором И.В. Анциферовой от 05.02.2019;
- Список методических указаний, используемых в образовательном процессе представлен в п. 10;
- Оценочные средства, представленные в рабочей программе дисциплины.

Привязка оценочных средств к контролируемым компетенциям, модулям, разделам (темам) дисциплины приведена в таблице.

№ п/п	Контролируемые модули,	Код контролируемой	Оценочные средства	

	разделы (темы) дисциплины	компетенции (или её части)	текущий контроль по дисциплине	промежуточная аттестация по дисциплине	Способ контроля
1	Тема 1	ОПК-1 ПК-32 ПК-34	Тесты, отчеты по практических работам	Вопросы и задания к зачету	Устно, письменно (тесты)
2	Тема 2	ОПК-1 ПК-32 ПК-34	Тесты, отчеты по практических работам	Вопросы и задания к зачету	Устно, письменно (тесты)
3	Тема 3	ОПК-1 ПК-32 ПК-34	Тесты, отчеты по практических работам	Вопросы и задания к зачету	Устно, письменно (тесты)
4	Тема 4	ОПК-1 ПК-32 ПК-34	Тесты, отчеты по практических работам	Вопросы и задания к зачету	Устно, письменно (тесты)
5	Тема 5	ОПК-1 ПК-32 ПК-34	Тесты, отчеты по практических работам	Вопросы и задания к зачету	Устно, письменно (тесты)
6	Тема 6	ОПК-1 ПК-32 ПК-34	Тесты, отчеты по практических работам	Вопросы и задания к зачету	Устно, письменно (тесты)
7	Тема 7	ПК-32 ПК-34 ПК-35	Тесты, отчеты по практических работам	Вопросы и задания к зачету	Устно, письменно (тесты)
8	Тема 8	ПК-32 ПК-34 ПК-35	Тесты, отчеты по практических работам	Вопросы и задания к зачету	Устно, письменно (тесты)
9	Тема 9	ОПК-1 ПК-32 ПК-34	Тесты, отчеты по практических работам	Вопросы и задания к зачету	Устно, письменно (тесты)

8. Основная и дополнительная литература, необходимая для освоения дисциплины

8.1 Основная литература

1. Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс] / В.Ф. Шаньгин. — Электрон. текстовые данные. — Саратов: Профобразование, 2017. — 702 с. — 978-5-4488-0070-2. — Режим доступа: http://www.iprbookshop.ru/63594.html

2. Федоров, В. В. Информационные технологии в юридической деятельности таможенных органов [Электронный ресурс] : учебник / В. В. Федоров. — Электрон. текстовые данные. — СПб. : Интермедия, 2017. — 480 с. — 978-5-4383-0083-0. — Режим доступа: http://www.iprbookshop.ru/82247.html

8.2 Дополнительная литература

1. Сычев Ю.Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов [Электронный ресурс] : учебное пособие / Ю.Н. Сычев. — Электрон. текстовые данные. — Саратов: Вузовское образование, 2018. — 195 с. — 978-5-4487-0128-3. — Режим доступа: http://www.iprbookshop.ru/72345.html

2. Фороузан Бехроуз А. Криптография и безопасность сетей [Электронный ресурс] : учебное пособие / БехроузА. Фороузан. — Электрон. текстовые данные. — Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское

образование, 2017. — 782 c. — 978-5-4487-0143-6. — Режим доступа: http://www.iprbookshop.ru/72337.html
3. Фомин Д.В. Информационная безопасность и защита информации: специализированные аттестованные программные и программно-аппаратные средства [Электронный ресурс] : учебно-методическое пособие / Д.В. Фомин. — Электрон. текстовые данные. — Саратов: Вузовское образование, 2018. — 218 c. — 978-5-4487-0297-6. — Режим доступа: http://www.iprbookshop.ru/77317.html

9. Ресурсы информационно – телекоммуникационной сети «Интернет», необходимые для освоения дисциплины

http://www.cyberpolice.ru (Web-сервер подразделения по выявлению и пресечению преступлений, совершаемых с использованием поддельных кредитных карт, и преступлений, совершаемых путем несанкционированного доступа в компьютерные сети и базы данных)
http://www.infosecurity. report.ru/ (портал по информационной безопасности)
http://www.void.ru/ (портал по информационной безопасности)
http://www.infosec.ru/ (Сервер компании НИП «Информзащита»)
http://www.jetinfo.ru/ (Информационный бюллетень «Jet Info» с тематическим разделом по информационной безопасности)
http://pdfcreator.ru/ (Официальный сайт программы PDFCreator)
http://en.protectorion.com/ (Официальный сайт программы Protectorion ToGo)
http://www.piriform.com/recuva (Официальный сайт программы Recuva)
http://www.handyrecovery.ru/ (Официальный сайт программы Handy Recovery)
http://www.pandorarecovery.com/local/ru/ (Официальный сайт программы Pandora Recovery)
http://www.drweb.ru/ (Официальный сайт программы Dr.Web)
http://www.consultant.ru/ (Официальный сайт компании «Консультант Плюс»)

10. Методические указания для обучающихся по освоению дисциплины

Работа на лекции является очень важным видом студенческой деятельности для изучения дисциплины «Информационная безопасность в таможенных органах». Краткие записи лекций (конспектирование) помогает усвоить материал. Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Конспект лучше подразделять на пункты, параграфы, соблюдая красную строку.

Принципиальные места, определения, формулы следует сопровождать замечаниями: «важно», «особо важно», «хорошо запомнить» и т.п. или подчеркивать красной ручкой. Целесообразно разработать собственную символику, сокращения слов, что позволит сконцентрировать внимание обучающегося на важных сведения. Прослушивание и запись лекции можно производить при помощи современных устройств (диктофон, ноутбук, нетбук и т.п.).

Работая над конспектом лекций, всегда следует использовать не только учебник, но и ту литературу, которую дополнительно рекомендовал лектор. По результатам работы с конспектом лекции следует обозначить вопросы, термины, материал, который вызывают трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии. Лекционный материал является базовым, с которого необходимо начать освоение соответствующего раздела или темы.

Методические указания по выполнению практических занятий

Проработка рабочей программы дисциплины, уделяя особое внимание целям и задачам, структуре и содержанию дисциплины.

Ознакомление с темами и планами практических (семинарских) занятий. Конспектирование источников. Подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы. Прослушивание аудио- и видеозаписей по заданной теме,

решение задач. Устные выступления обучающихся по контрольным вопросам семинарского занятия.

Выступление на семинаре должно быть компактным и вразумительным, без неоправданных отступлений и рассуждений. Обучающийся должен излагать (не читать) материал выступления свободно. Необходимо концентрировать свое внимание на том, что выступление должно быть обращено к аудитории, а не к преподавателю, т.к. это значимый аспект профессиональных компетенций бакалавров.

По окончании семинарского занятия обучающемуся следует повторить выводы, сконструированные на семинаре, проследив логику их построения, отметив положения, лежащие в их основе. Для этого обучающемуся в течение семинара следует делать пометки. Более того в случае неточностей и (или) непонимания какого-либо вопроса пройденного материала обучающемуся следует обратиться к преподавателю для получения необходимой консультации и разъяснения возникшей ситуации.

Методические указания по выполнению самостоятельной работы

Самостоятельная работа проводится с целью: систематизации и закрепления полученных теоретических знаний и практических умений обучающихся; углубления и расширения теоретических знаний обучающихся; формирования умений использовать нормативную, правовую, справочную документацию, учебную и специальную литературу; развития познавательных способностей и активности обучающихся: творческой инициативы, самостоятельности, ответственности, организованности; формирование самостоятельности мышления, способностей к саморазвитию, совершенствованию и самоорганизации; формирования профессиональных компетенций; развитию исследовательских умений обучающихся.

Формы и виды самостоятельной работы обучающихся: чтение основной и дополнительной литературы – самостоятельное изучение материала по рекомендуемым литературным источникам; выполнение разноуровневых заданий, работа со словарем, справочником; поиск необходимой информации в сети Интернет; конспектирование источников; реферирование источников; подготовка к различным формам текущей и промежуточной аттестации (к тестированию, зачету); выполнение домашних контрольных работ; самостоятельное выполнение практических заданий репродуктивного типа (ответы на вопросы, задачи, тесты; выполнение творческих заданий).

Технология организации самостоятельной работы обучающихся включает использование информационных и материально-технических ресурсов образовательного учреждения: библиотеку с читальным залом, укомплектованную в соответствии с существующими нормами; учебно-методическую базу учебных кабинетов, лабораторий и зала кодификации; компьютерные классы с возможностью работы в Интернет; аудитории (классы) для консультационной деятельности; учебную и учебно-методическую литературу, разработанную с учетом увеличения доли самостоятельной работы обучающихся, и иные методические материалы.

Перед выполнением обучающимися внеаудиторной самостоятельной работы преподаватель проводит консультирование по выполнению задания, который включает цель задания, его содержания, сроки выполнения, ориентировочный объем работы, основные требования к результатам работы, критерии оценки. Во время выполнения обучающимися внеаудиторной самостоятельной работы и при необходимости преподаватель может проводить индивидуальные и групповые консультации.

Самостоятельная работа может осуществляться индивидуально или группами обучающихся в зависимости от цели, объема, конкретной тематики самостоятельной работы, уровня сложности, уровня умений обучающихся.

Контроль самостоятельной работы обучающихся предусматривает: соотнесение содержания контроля с целями обучения; объективность контроля; валидность контроля (соответствие предъявляемых заданий тому, что предполагается проверить); дифференциацию контрольно- измерительных материалов.

Формы контроля самостоятельной работы: просмотр и проверка выполнения самостоятельной работы преподавателем; организация самопроверки, взаимопроверки выполненного задания в группе; обсуждение результатов выполненной работы на занятии; проведение письменного опроса; проведение устного опроса; организация и проведение индивидуального собеседования; организация и проведение собеседования с группой; защита отчетов о проделанной работе.

Методические указания по выполнению тестовых заданий

Тест - это система стандартизированных вопросов (заданий) позволяющих автоматизировать процедуру измерения уровня знаний и умений обучающихся. Тесты могут быть аудиторными и внеаудиторными. О проведении теста, его формы, а также раздел (темы) дисциплины, выносимые на тестирование, доводит до сведения обучающихся преподаватель, ведущий семинарские занятия. Тестирование ставит целью оценить уровень освоения обучающимися дисциплины в целом, либо её отдельных тем, а также знаний и умений, предусмотренных компетенциями. Тестирование проводится для обучающихся всех форм обучения в письменной либо компьютерной форме. Соответственно, тестовые задания могут быть либо на бумажных носителях, либо в компьютерной программе. Сама процедура тестирования занимает часть учебного занятия (10 минут). Для выполнения тестовых заданий обучающийся должен повторить теоретический материал, изложенный на лекциях и рассмотренный на практических занятиях.

Методические указания по написанию доклада

Доклад – это один из видов монологической речи, публичное, развернутое сообщение по определенному вопросу, основанное на привлечении документальных данных. Цель доклада – передача информации от обучающегося аудитории. Отличительной чертой доклада является использование документальных источников, которые ложатся в основу устного или письменного сообщения. Тема доклада должна быть либо заглавной в проблематике всего семинара, либо дополнять содержание основных учебных вопросов, либо посвящаться обзору какой-либо публикации, статистического материала и т.д., имеющих важное значение для раскрытия обсуждаемых вопросов семинара и формирования необходимых компетенций выпускника.

После выбора темы доклада составляется перечень источников (монографий, научных статей, справочной литературы, содержащей комментарии, результаты социологических исследований и т.п.). Содержание материала должно быть логичным, изложение материала носит проблемно-поисковый характер.

Примерные этапы работы над докладом: формулирование темы (тема должна быть актуальной, оригинальной и интересной по содержанию); подбор и изучение основных источников по теме; составление библиографии; обработка и систематизация информации; разработка плана; написание доклада; публичное выступление с результатами исследования на семинаре. Доклад должен отражать: знание современного состояния проблемы; обоснование выбранной темы; использование известных результатов и фактов; полноту цитируемой литературы, ссылки на работы ученых, занимающихся данной проблемой; актуальность поставленной проблемы; материал, подтверждающий научное, либо практическое значение в настоящее время.

Выступление с докладом продолжается в течение 5-7 минут по плану. Выступающему обучающемуся, по окончании представления доклада, могут быть заданы вопросы по теме доклада. Рекомендуемый объем 3-5 страниц компьютерного (машинописного) текста. К докладу обучающийся готовится самостоятельно, определив предварительно с преподавателем тему доклада, а также проработав вопрос о его структуре. Необходимо обращение к специальной литературе по теме доклада, в том числе и литературе, не указанной в данной рабочей программе. Если в процессе подготовки доклада у обучающегося возникают затруднения, они могут быть разрешены на консультации с преподавателем.

По наиболее сложным вопросам на доклад может быть отведено и более продолжительное время. В обсуждении докладов принимают участие все присутствующие на семинаре обучающиеся.

Методические указания по решению разноуровневых задач

Обдумывание и обсуждение ответов на задания разного уровня:

а) репродуктивного уровня, позволяющие оценивать и диагностировать знание фактического материала (базовые понятия, алгоритмы, факты) и умение правильно использовать специальные термины и понятия, узнавание объектов изучения в рамках определенного раздела дисциплины;

б) реконструктивного уровня, позволяющие оценивать и диагностировать умения синтезировать, анализировать, обобщать фактический и теоретический материал с формулированием конкретных выводов, установлением причинно-следственных связей;

в) творческого уровня, позволяющие оценивать и диагностировать умения, интегрировать знания различных областей, аргументировать собственную точку зрения.

Методические рекомендации по написанию и оформлению рефератов

Реферат (лат.refero - доношу, сообщаю, излагаю) – это краткое изложение содержания научной работы, книги, учения, оформленное в виде письменного публичного доклада; доклад на заданную тему, сделанный на основе критического обзора соответствующих источников информации (научных трудов, литературы по теме). Реферат является адекватным по смыслу изложением содержания первичного текста и отражает главную информацию первоисточника. Реферат должен быть информативным, объективно передавать информацию, отличаться полнотой изложения, а также корректно оценивать материал, содержащийся в первоисточнике.

Различают два вида рефератов: продуктивные и репродуктивные.

Репродуктивный реферат воспроизводит содержание первичного текста. Продуктивный содержит творческое или критическое осмысление реферируемого источника. Репродуктивные рефераты можно разделить еще на два вида: реферат-конспект и реферат-резюме. Реферат-конспект содержит фактическую информацию в обобщенном виде, иллюстрированный материал, различные сведения о методах исследования, результатах исследования и возможностях их применения. Реферат-резюме содержит только основные положения данной темы.

Среди продуктивных рефератов выделяются рефераты-доклады и рефераты-обзоры. Реферат-обзор составляется на основе нескольких источников и сопоставляет различные точки зрения по данному вопросу. В реферате-докладе наряду с анализом информации первоисточника, есть объективная оценка проблемы; этот реферат имеет развернутый характер.

Реферат оформляется в соответствии с ГОСТ Р 7.05-2008 (Библиографическая ссылка); ГОСТ 7.32-2001 (Отчет о научно-исследовательской работе); ГОСТ 7.1-2003 (Библиографическая запись. Библиографическое описание. Общие требования и правила составления); ГОСТ 2.105-95 (Общие требования к текстовым документам) и их актуальных редакций.

Реферат выполняется на листах формата А4 (размер 210 на 297 мм) с размерами полей: верхнее– 20 мм, нижнее – 20 мм, правое – 15мм, левое – 30 мм. Шрифт Times New Roman, 14 пт, через полуторный интервал. Абзацы в тексте начинают отступом равным 1,25 см.

Текст реферата следует печатать на одной стороне листа белой бумаги. Цвет шрифта должен быть черным. Заголовки (располагаются в середине строки без точки в конце и пишутся строчными буквами, с первой прописной, жирным шрифтом. Текст реферата должен быть выровнен по ширине. Нумерация страниц реферата выполняется арабскими цифрами сверху посередине, с соблюдением сквозной нумерации по всему тексту. Нумерация страниц начинается с титульного листа, но номер страницы на титульном листе не ставится.

Реферат строится в указанной ниже последовательности: титульный лист; содержание; введение; основная часть; заключение; список использованных источников и литературы; приложения (если есть). Общий объем реферат не должен превышать 20 листов.

Методические указания по подготовке к зачету

Зачет проводится с записью «зачтено» в зачетной книжке. Залогом успешной сдачи зачета является систематические, добросовестные занятия обучающегося. Специфической задачей обучающегося в период сессии являются повторение, обобщение и систематизация всего материала, который изучен в течение года.

При подготовке к зачету необходимо ориентироваться на конспекты лекций, рабочую программу дисциплины, нормативную, учебную и рекомендуемую литературу.

Основное в подготовке к сдаче зачету - это повторение всего материала дисциплины, по которому необходимо сдавать зачет. При подготовке к сдаче зачета обучающийся весь объем работы должен распределять равномерно по дням, отведенным для подготовки к зачету, контролировать каждый день выполнение намеченной работы.

По завершению изучения дисциплины сдается зачет.

В период подготовки к зачету обучающийся вновь обращается к уже изученному (пройденному) учебному материалу.

Подготовка обучающегося к зачету включает в себя три этапа: самостоятельная работа в течение семестра; непосредственная подготовка в дни, предшествующие зачету по темам курса; подготовка к ответу на задания, содержащиеся в билетах (тестах) зачета.

Зачет проводится по вопросам (тестам), охватывающим весь пройденный материал дисциплины, включая вопросы, отведенные для самостоятельного изучения.

Для успешной сдачи зачета по дисциплине «Информационная безопасность в таможенных органах» обучающиеся должны принимать во внимание, что все основные категории курса, которые указаны в рабочей программе, нужно знать, понимать их смысл и уметь его разъяснить; указанные в рабочей программе формируемые профессиональные компетенции в результате освоения дисциплины должны быть продемонстрированы обучающимся; семинарские занятия способствуют получению более высокого уровня знаний и, как следствие, более высокой оценке на зачете; готовиться к зачету необходимо начинать с первой лекции и первого семинара. При подготовке к зачету необходимо ориентироваться на конспекты лекций, рекомендуемую литературу и др.

11. Информационные технологии, используемые при осуществлении образовательного процесса (включая программное обеспечение и информационные справочные системы)

11.1 Перечень информационных технологий, используемых при осуществлении образовательного процесса

№ п/п	Наименование раздела (темы) дисциплины (модуля)	Информационные технологии
1	Информационная безопасность таможенных органов в системе национальной безопасности Российской Федерации.	Использование слайд-презентаций «Введение в информационную безопасность» при проведении лекционных, практических занятий
2	Национальные интересы таможенных органов в информационной сфере и их обеспечение.	Использование слайд-презентаций «Введение в информационную безопасность» при проведении лекционных, практических занятий
3	Виды угроз информационной безопасности таможенных органов.	Использование слайд-презентаций «Введение в информационную безопасность» при проведении лекционных, практических занятий
4	Источники угроз	Использование слайд-презентаций «Введение в

	информационной безопасности таможенных органов.	информационную безопасность», при проведении лекционных, практических занятий
5	Информационная безопасность и информационное противоборство.	Использование слайд-презентаций «Введение в информационную безопасность» при проведении лекционных, практических занятий
6	Обеспечение информационной безопасности объектов информатизационной сферы таможенных органов в условиях информационной войны.	Использование слайд-презентаций «Введение в криптографию» при проведении лекционных, практических занятий
7	Общие методы обеспечения информационной безопасности таможенных органов.	Использование слайд-презентаций «Сети ЭВМ и защита информации» при проведении лекционных, практических занятий
8	Основы комплексного обеспечения информационной безопасности таможенных органов.	Использование слайд-презентаций «Защита информации в компьютерных системах» при проведении лекционных, практических занятий
9	Методы и средства обеспечения информационной безопасности компьютерных систем таможенных органов.	Использование слайд-презентаций «Защита информации в компьютерных системах» при проведении лекционных, практических занятий

11.2 Перечень программного обеспечения, информационных справочных систем, используемого при осуществлении образовательного процесса

1. Справочная правовая система Консультант Плюс - договор №21/2018/К/Пр от 09.01.2018;
2. Microsoft Windows 7 Starter предустановленная лицензионная;
3. Micrososoft Windows Vista Business Russian Upgrade Academik OPEN No Level; Лицензия № 42859743, Лицензия № 42117365;
4. Micrososoft Office Professional Plus 2007 Russian Academik OPEN No Level; Лицензия № 42859743, Лицензия № 42117365;
5. Micrososoft Office Professional Plus 2007 Russian Academik OPEN No Level; Лицензия № 42859743;
6. Программное обеспечение: ВЭД-Декларант; ВЭД-Контроль; ВЭД-Инфо; ВЭД-Алфавит; Лицензионный договор №ЛУ-2308/1901 от 30.08.2019.

12. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине:

Учебные занятия по дисциплине «Информационная безопасность в таможенных органах» проводятся в учебных кабинетах, оснащенных соответствующим оборудованием и программным обеспечением:

Наименование специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы
305009, г. Курск, ул. Интернациональная, д.6-б. Учебная аудитория №19 для проведения занятий лекционного и семинарского типа; групповых и индивидуальных консультаций; текущего контроля и	Рабочие места студентов: стулья, парты. Рабочее место преподавателя: стол, стул, кафедра, аудиторная меловая доска, проектор BenQ Projector MP515, экран для проектора. Наборы демонстрационного оборудования и учебно-наглядных пособий: Карта

промежуточной аттестации.	Российской Федерации. Российская Федерация. Федеративное устройство; герб Российской Федерации, герб Курской области; информационные стенды: «Правовое регулирование деятельности таможенных органов», «Государственное регулирование внешнеторговой деятельности».
305009 , г. Курск ул. Интернациональная, д. 6-б. Учебная аудитория № 29 для проведения занятий лекционного и семинарского типа; выполнения курсовых работ, групповых и индивидуальных консультаций; текущего контроля и промежуточной аттестации, помещение для самостоятельной работы; помещение для хранения и профилактического обслуживания учебного оборудования.	Рабочие места студентов: стулья, парты. Рабочее место преподавателя: стол, стул, кафедра, аудиторная меловая доска, проектор BenQ Projector MP515, экран для проектора. Наборы демонстрационного оборудования и учебно-наглядных пособий: Политическая карта мира, Герб Российской Федерации, герб Центрального таможенного управления, герб Федеральной Таможенной службы Российской Федерации, флаги Российской Федерации; информационные стенды: «Государственная служба», «INCOTERMS 2010», «Транспортная инфраструктура России», Тренажер электронного декларирования, знак обозначения пределов зоны таможенного контроля, шкаф с демонстрационным материалом: запорно-пломбировочные устройства различных видов, образцы товаросопроводительных документов, досмотровое зеркало. Монитор LCD Monitor 17” Acer AL1716Fs-14 шт. Компьютер Intel Pentium Dual CPU E2140- 10 шт. Клавиатура – 14шт. Мышь- 14 шт. Имеется локальная сеть. Имеется доступ в Интернет на всех ПК.
305009, г. Курск, ул. Интернациональная, д.6-б. Учебная аудитория №15 помещение для самостоятельной работы.	Рабочие места студентов: стулья, парты. Нетбук ASUS-X101CH – 10 шт. Имеется локальная сеть. Имеется доступ в Интернет на всех ПК.
305009, г. Курск, ул. Интернациональная, д.6-б. Учебная аудитория №28-а помещение для хранения и профилактического обслуживания учебного оборудования.	