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
«05» июля 2023 г.

Рабочая программа дисциплины
«Организационно-правовые основы информационной безопасности»

Направление подготовки: 40.03.01 Юриспруденция
Направленность (профиль) подготовки: «Правовое регулирование государственного и муниципального управления»
Уровень подготовки: бакалавриат
Форма обучения: очная
Год начала подготовки по УП: 2020

Курск, 2023

1. Цели и задачи освоения дисциплины

Цель дисциплины — обучить студентов принципам обеспечения информационной безопасности государства, подходам к анализу его информационной инфраструктуры и решению задач обеспечения информационной безопасности компьютерных систем»; раскрыть основы правового регулирования отношений в информационной сфере, конституционные гарантии прав граждан на получение информации и механизм их реализации, понятия и виды защищаемой информации по законодательству РФ, систему защиты государственной тайны, основы правового регулирования отношений в области интеллектуальной собственности и способы защиты этой собственности, а также понятие и виды компьютерных преступлений.

Задачи дисциплины – дать основы:

- обеспечения информационной безопасности государства;
- 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;
- информационного законодательства Российской Федерации;
- системы защиты государственной тайны;
- правил лицензирования и сертификации в области защиты информации;
- международного законодательства в области защиты информации;
- знаний о компьютерных преступлениях.

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

В результате изучения курса студенты должны:

Знать:

- способы сбора, передачи, хранения информации;
- основные понятия и общеметодологические принципы теории информационной безопасности;
- роль информационной безопасности в обеспечении национальной безопасности государства;
- основные методы нарушения конфиденциальности, целостности и доступности информации.
- основные причины, виды, каналы утечки и искажения информации;
- основные направления обеспечения информационной безопасности объектов информационной сферы государства в условиях информационной войны;
- содержание основных понятий по правовому обеспечению информационной безопасности;
- правовые способы защиты государственной тайны, конфиденциальной информации и интеллектуальной собственности;
- понятие и виды защищаемой информации, особенности государственной тайны как вида защищаемой информации;
- основы правового регулирования взаимоотношений администрации и персонала в области защиты информации;
- правила лицензирования и сертификации в области защиты информации;
- виды и признаки компьютерных преступлений, особенности основных следственных действий при расследовании указанных преступлений.

Уметь:

- подбирать и использовать соответствующие правовые, организационно-технические и экономические методы обеспечения информационной безопасности

выбранных объектов;

– отыскивать необходимые нормативные правовые акты и информационно-правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации;

– применять действующую законодательную базу в области информационной безопасности;

– разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов.

Владеть:

– навыками анализа информационной инфраструктуры государства;

– навыками формальной постановки и решения задачи обеспечения информационной безопасности выбранного объекта телекоммуникационной системы;

– понятиями информационного права как основы информационного общества;

– об информационном праве как основе информационного общества.

Компетенции обучающегося, формируемые в результате освоения дисциплины «Организационно-правовые основы информационной безопасности»:

ОК-3 - владение основными методами, способами и средствами получения, хранения, переработки информации, навыками работы с компьютером как средством управления информацией;

ОК-4 - способность работать с информацией в глобальных компьютерных сетях;

ОК-7 - способность к самоорганизации и самообразованию.

ПК-3 - способность обеспечивать соблюдение законодательства Российской Федерации субъектами права

3. Место дисциплины в структуре образовательной программы

Дисциплина «Организационно-правовые основы информационной безопасности» относится к дисциплинам по выбору. «Организационно-правовые основы информационной безопасности» поддерживает межпредметные связи с дисциплинами «Информационное право», «Правовая информация и основы документооборота в юридической практике», «Информационные технологии в юридической деятельности».

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)	
	1 курс, 2 семестр	Всего
Общая трудоемкость	2 (72)	2 (72)
Контактная работа	1,18 (42,3)	1,18 (42,3)
лекции практические (семинарские) занятия контактная работа на промежуточную аттестацию	0,38 (14) 0,77 (28) 0,01 (0,3)	0,38 (14) 0,77 (28) 0,01 (0,3)
Самостоятельная работа	0,82 (29,7)	0,82 (29,7)
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 трудоемкости	В том числе контактная работа					Сам. (инд.) раб.
			Всего/ в интерактивной форме	Лекций	Практ. (семин.) занятий	Лабор. занятий	Атт. контакт. работа	
1	Информационная безопасность в системе национальной безопасности Российской Федерации. Национальные интересы Российской Федерации в информационной сфере и их обеспечение.	6	2	2	-			4
2	Виды угроз информационной безопасности Российской Федерации. Источники угроз информационной безопасности.	6	2	2	-			4
3	Информационная безопасность и информационное противоборство.	6	2	2	-			4
4	Обеспечение информационной безопасности объектов информатизационной сферы государства в условиях информационной войны.	16	12	2	10			4
5	Общие методы обеспечения информационной безопасности Российской Федерации.	16	12/4	2	10			4

№	Наименование раздела (темы)	Всего часов в трудоемкости	В том числе контактная работа					Сам. (инд.) раб.
			Всего/ в интерактивной форме	Лекций	Практ. (семин.) занятий	Лабор. занятий	Атт. контакт. работа	
6	Законодательство РФ в области информационной безопасности. Правовой режим защиты государственной тайны. Правовые режимы защиты конфиденциальной информации.	5,7	2/2	2	-			3,7
7	Лицензирование и сертификация в информационной сфере. Защита интеллектуальной собственности. Компьютерные правонарушения.	4	2	2	-			2
8	Международное законодательство в области защиты информации. Организационное обеспечение.	2			-			2
9	Методы и средства обеспечения информационной безопасности компьютерных систем	10	8		8			2
	Контактная работа на промежуточную аттестацию	0,3	0,3				0,3	
	Всего	**72**	**42,3/6**	**14**	**28**		**0,3**	**29,7**

.

5.2 Содержание семинарских (практических) занятий

ПРАКТИЧЕСКОЕ (СЕМИНАРСКОЕ) ЗАНЯТИЕ № 1: Обеспечение информационной безопасности объектов информатизационной сферы государства в условиях информационной войны

Цель работы: изучить методы передачи скрытой информации.

Контрольные вопросы

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

Форма проведения и контроля: устный опрос, доклады, практические работы, тестирование

ПРАКТИЧЕСКОЕ (СЕМИНАРСКОЕ) ЗАНЯТИЕ № 2: Общие методы обеспечения информационной безопасности Российской Федерации.
Цель работы: Изучить механизмы создания защищенных PDF файлов.

Контрольные вопросы

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?

Форма проведения и контроля: устный опрос, доклады, практические работы, тестирование, презентация

ПРАКТИЧЕСКОЕ (СЕМИНАРСКОЕ) ЗАНЯТИЕ № 3: Методы и средства обеспечения информационной безопасности компьютерных систем.
Восстановление удаленных файлов
Цель работы: Изучить методы восстановления файлов с данными.

Контрольные вопросы

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?

Форма проведения и контроля: устный опрос, доклады, презентация

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.

1.Самостоятельное изучение теоретического курса

1. Ознакомиться с основной и дополнительной литературой по программе дисциплины.
2. Дополнение конспектов лекций (по основной и дополнительной литературе).
3. Подготовка к практическим и лабораторным занятиям (ознакомление с методическими рекомендациями, повторение теории и выполнение подготовительных заданий, ведение протокола и оформление отчета по лабораторным работам).
4. Подготовка сообщений (докладов) по отдельным вопросам.

2.Задания на самостоятельную работу обучаемых

1. Ознакомиться с основной и дополнительной литературой по программе дисциплины.
2. Дополнение конспектов лекций и отчётов по лабораторным занятиям (по основной и дополнительной литературе).
3. Подготовка к лабораторным занятиям (ознакомление с методическими рекомендациями, повторение теории и выполнение подготовительных заданий, ведение протокола и оформление отчёта по лабораторным работам).
4. Подготовка к тестам на различных этапах семестра. Работа над ошибками после проверки тестов.
5. Посещение выставок по вычислительной технике, оформление отчёта о них.
6. Изучение рекламы и прайс-листов по программному обеспечению в области баз данных.
7. Поиск новинок и планов развития техники по периодической литературе в области баз данных.
8. Совершенствование навыков работы с клавиатурой по набору текстовой информации и её стандартному представлению (воспитательный аспект).
9. Подготовка сообщений (докладов) по отдельным вопросам.

Примерная тематика учебно-исследовательских заданий

1. «Владелец сертификата ключа подписи» в соответствии с Федеральным законом от 10 января 2002 г. № 1-ФЗ "Об электронной цифровой подписи"
2. Определение термина «коммерческая тайна» на основе Федерального закона «О коммерческой тайне» и ст. 139 ГК РФ. Группы баз данных отнесенные к коммерческой тайне.
3. Основные понятия, используемые в Федеральном законе от 27.07.2006 г . № 149-ФЗ «Об информации, информационных технологиях и защите информации» (далее ФЗ «Об информации»).
4. Ограничение доступа к информации на основании ст. 9 ФЗ «Об информации».
5. Специальные категории персональных баз данных в соответствии с ФЗ «О персональных данных».
6. Дать определение терминам «Аналоговые данные», «Аналоговый документ; АнД (аналоговая форма документа)», в соответствии с ГОСТ Р 52292-2004. Информационная технология. Электронный обмен информацией. Термины и определения.
7. Дать определение «данные» в соответствии с ГОСТ Р 52292-2004. Информационная технология. Электронный обмен информацией.

8. Дать определения терминов «Администратор автоматизированной системы (администратор АС)», «Администратор защиты», «Администратор базы данных». Различие и единство данных терминов.

9. Назовите основные направления мер защиты информации на основании ст.16. ФЗ «Об информации».

10. Права субъекта персональных данных – физического лица в соответствии с ФЗ «О Персональных данных»

11. Жизненный цикл автоматизированной системы (АС) в соответствии с ГОСТ 34.003-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы.

12. Дать определение терминов «Аутентичный документ», «Атрибут», в соответствии с ГОСТ 2.051-2006. Единая система конструкторской документации. Электронные документы. Общие положения

13. Идентичность данных в соответствии с ГОСТ Р 51170-98. Качество служебной информации.

14. Кодекс Российской Федерации об административных правонарушениях (КоАП РФ) в области правил защиты информации (ст. 13.11, 13.12, 13.13, 13.14, 17.13).

15. Уголовный кодекс РФ (УК РФ) о компьютерных преступлениях (ст.272)

16. УК РФ о компьютерных преступлениях (ст. 273)

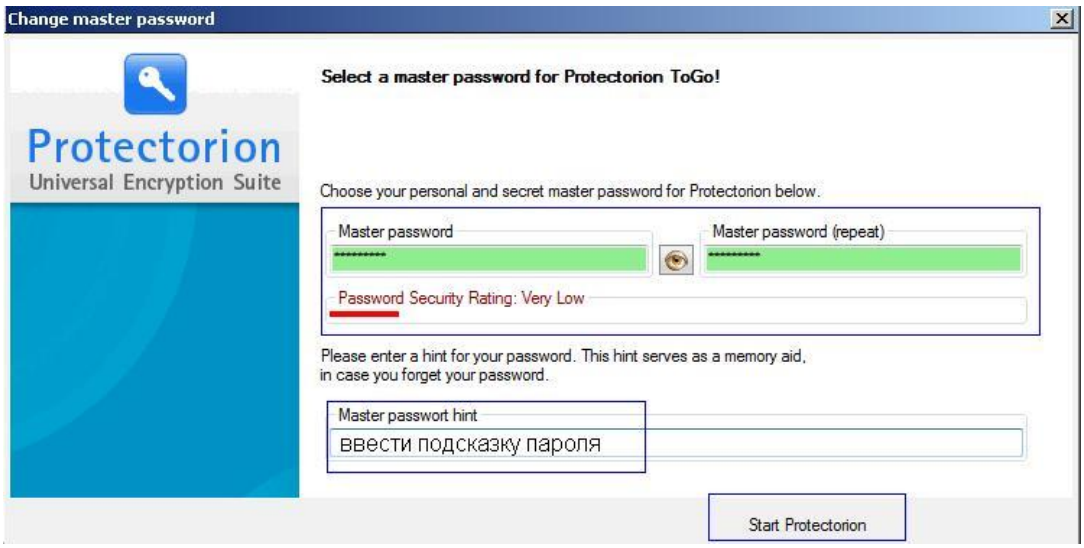
17. УК РФ о компьютерных преступлениях (ст.274)

18. УК РФ о преступлениях, связанных с получением и разглашением информации, составляющей коммерческую, налоговую или банковскую тайну

Задачи для самостоятельной работы

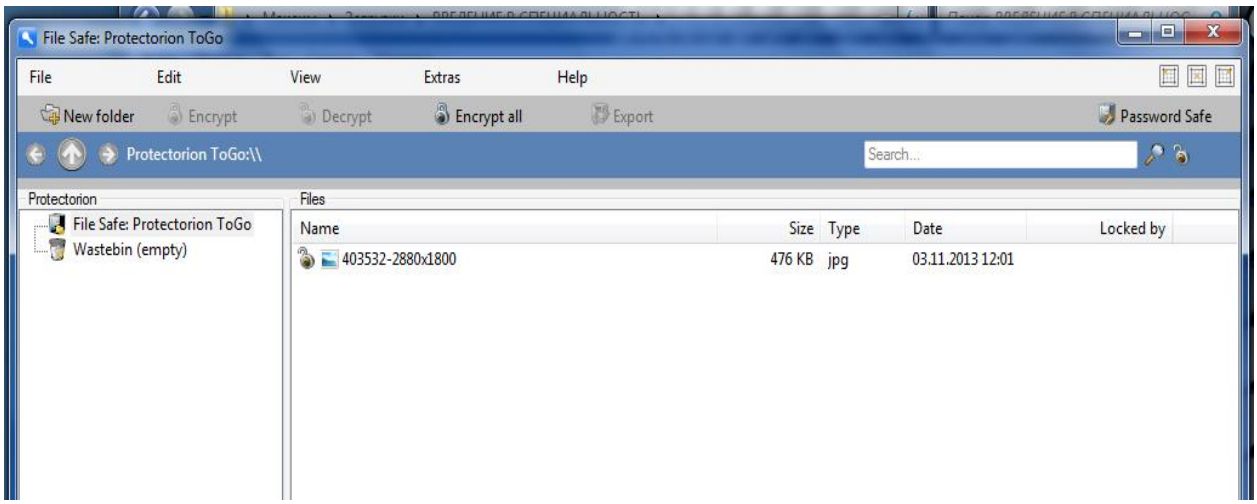
Задача I. Работа с программой Protectorion ToGo

1. Запускаем программу Protectorion ToGo. После первого запуска программа предложит ввести главный пароль, который будет использоваться для дальнейшего доступа к зашифрованным данным. Плюс к этому можно ввести подсказку, которая поможет вспомнить введенный пароль.



Окно для задания первоначальных параметров

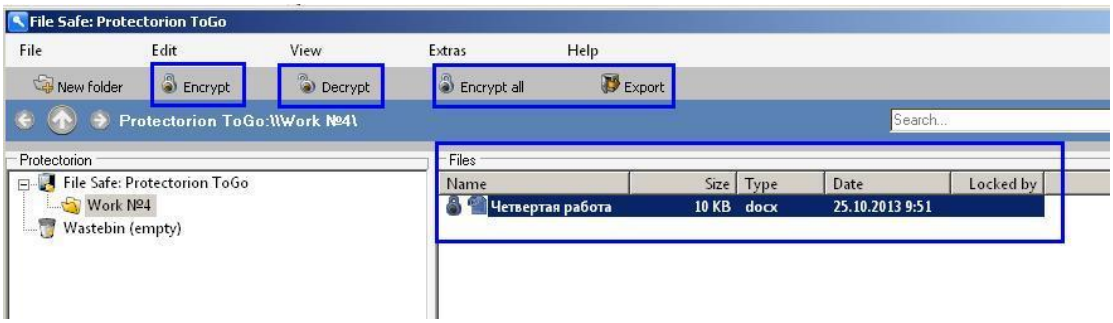
2. В главном окне Protectorion ToGo создаем папки с файлами путем обычного их переноса в свободную область. Структура папок отображается в виде дерева в левой части окна, а в правой части содержимое выбранной папки.



Интерфейс программы Protectorion ToGo

Просматривать и запускать фалы можно непосредственно из окна Protectorion ToGo как из обычного проводника Windows.

3. Для шифрации файла нажимаем кнопку «Encrypt» или всех файлов «Encrypt all».



Работа с файлами в программе Protectorion ToGo

4. Для снятия защиты с файлов и папок извлекаем их в выбранную папку при помощи кнопки «Extract».

Задача II. Работа с программой Simple File Encryptor

1. Запускаем программу Simple File Encryptor (рис. 20).

В главном меню программы есть 3 основные вкладки:

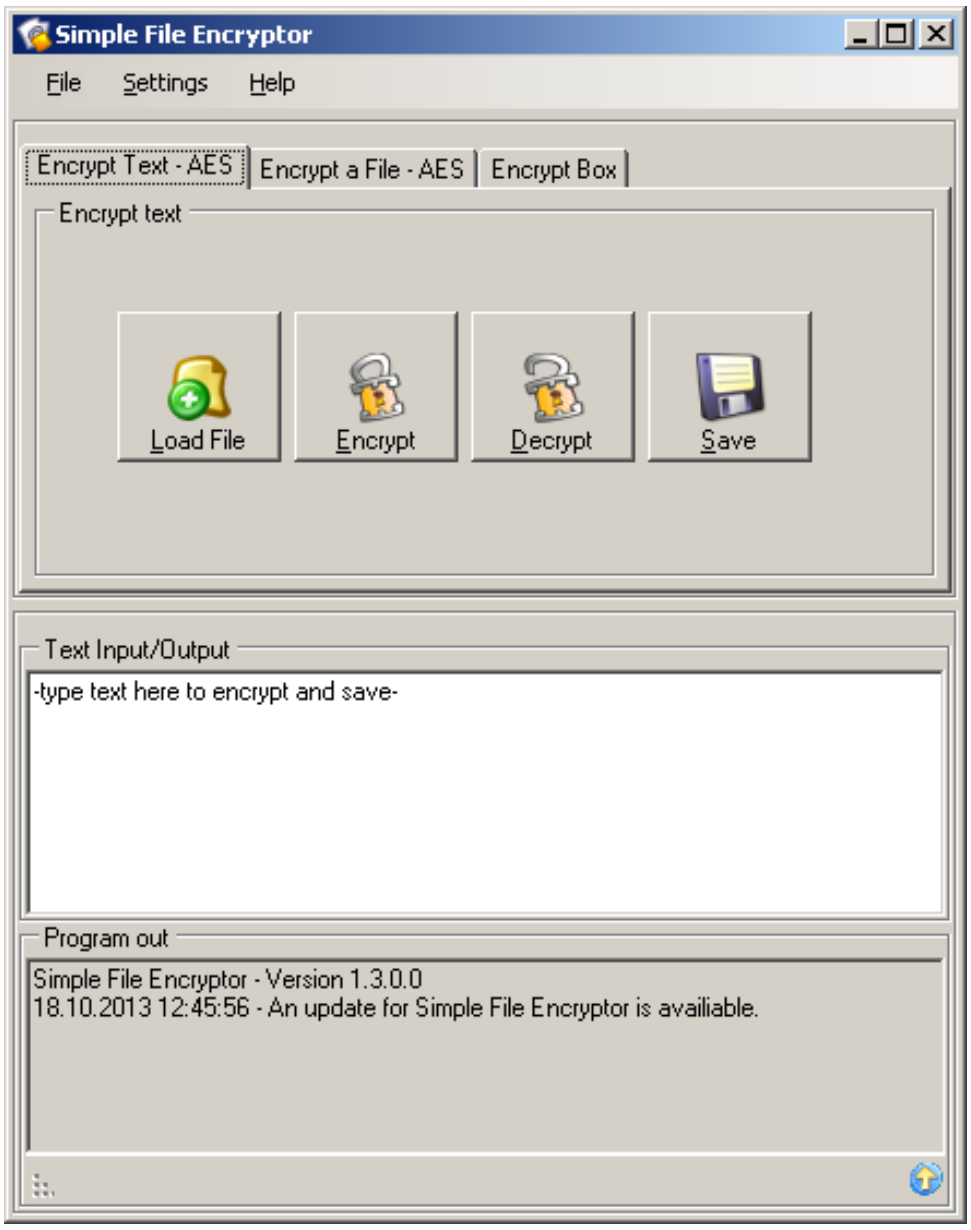
– «Encrypt Text – AES». Отвечает за шифрование текстового файла.

– «Encrypt a File –AES». Отвечает за шифрование файлов.

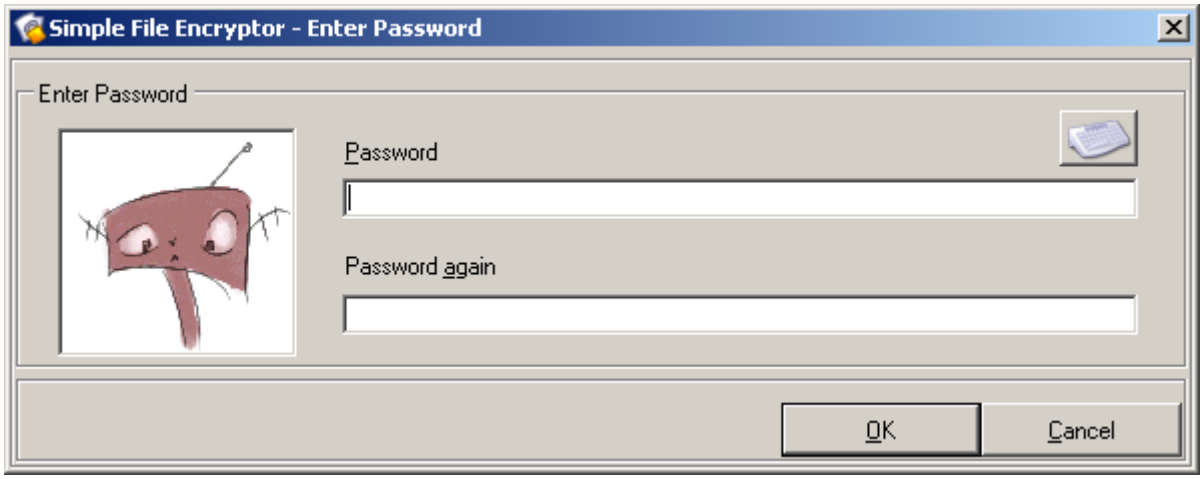
– «Encrypt Box». Отвечает за шифрование целых папок с файлами.

2. Для начала работы выберем, например, вкладку «Encrypt Text – AES», в этой вкладке нажмем кнопку «Load File», чтобы файл для шифрования. После указания файла нажмем кнопку «Encrypt».

3. После чего программа откроет новое окно, в котором предложит указать пароль для шифрования. Создаем криптостойкий пароль и вводим его в поля «Password» и «Password again» и нажимаем «Ok». Так же в этом окне можно использовать виртуальную клавиатуру, для защиты от программ кейлоггеров.



Интерфейс программы Simple File Encryptor



Окно для ввода пароля

4. После успешного шифрования, программа предложит сохранить результат или можно сохранить результат позже, при помощи кнопки «Save». Для это нужно будет указать путь для сохранения и дать имя файлу.

Получившийся файл будет иметь формат .aes.sfe_tx.

5. Для обратной расшифровки, в той же вкладке нажимаем кнопку «Load File», указываем раннее получившийся файл и нажимаем кнопку «Decrypt». Вводим установленный на файл пароль, после расшифровки сохраняем результат в указанную папку.

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?
13. Каковы особенности информации как объекта гражданско-правовых отношений?
14. Что такое документирование информации и почему оно является необходимым условием установления права собственности на информацию?
15. В чем заключаются особенности правового режима информационных ресурсов?
16. Возможны ли ограничения права собственности на информационные ресурсы?
17. Назовите условия возникновения права собственности на информационные ресурсы?
18. Раскройте понятие информации с ограниченным доступом.
19. Каковы особенности института коммерческой тайны?
20. В чем заключается механизм защиты коммерческой тайны?
21. Каковы современные проблемы защиты служебной тайны?
22. Что такое банковская тайна и в чем заключается специфика ее защиты?
23. Перечислите субъекты и объекты правоотношений в сфере защиты государственной тайны. Раскройте принципы засекречивания.
24. Каковы особенности механизма засекречивания?
25. Дайте сравнительный анализ механизмов засекречивания в России и США.
26. Каковы реквизиты носителей государственной тайны?
27. В чем заключаются особенности рассекречивания?

28. Какова система органов защиты государственной тайны, каковы основные правомочия включенных в нее органов государственной власти?
29. Перечислите основные правовые механизмы допуска граждан к государственной тайне.
30. В чем заключается и из чего состоит механизм распоряжения государственной тайной?
31. Перечислите признаки состава преступления и раскройте их понятие.
32. Каковы составы преступления, являющихся нарушением тайны сообщений и отказом в информации?
33. Какова уголовно-правовая защита конфиденциальной информации?
34. Дайте характеристику неправомерного доступа к компьютерной информации как уголовного преступления.
35. Каковы составы преступлений в части создания, использования и распространения вредоносных программ для ЭВМ?
36. В чем заключается нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети, как уголовного преступления?
37. Какими группами норм определяется уголовно-правовая защита государственной тайны?
38. Какова правовая основа функционирования систем лицензирования и сертификации в области защиты информации?
39. Перечислите уполномоченные органы лицензирования и их основные обязанности.
40. В чем заключаются особенности проведения специальных экспертиз?
41. Каковы особенности сертификации средств защиты информации?
42. Раскройте структуру государственной системы сертификации и полномочия центральных и федеральных органов.
43. В чем заключаются испытания средств защиты информации?
44. Опишите систему государственной аттестации руководителей и специалистов в области защиты информации.

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.

Примерная тематика докладов

1. «Владелец сертификата ключа подписи» в соответствии с Федеральным законом от 10 января 2002 г. № 1-ФЗ "Об электронной цифровой подписи"

2. Определение термина «коммерческая тайна» на основе Федерального закона «О коммерческой тайне» и ст. 139 ГК РФ. Группы баз данных отнесенные к коммерческой тайне.
3. Основные понятия, используемые в Федеральном законе от 27.07.2006 г . № 149-ФЗ «Об информации, информационных технологиях и защите информации» (далее ФЗ «Об информации»).
4. Ограничение доступа к информации на основании ст. 9 ФЗ «Об информации».
5. Специальные категории персональных баз данных в соответствии с ФЗ «О персональных данных».
6. Дать определение терминам «Аналоговые данные», «Аналоговый документ; АнД (аналоговая форма документа)», в соответствии с ГОСТ Р 52292-2004. Информационная технология. Электронный обмен информацией. Термины и определения.
7. Дать определение «данные» в соответствии с ГОСТ Р 52292-2004. Информационная технология. Электронный обмен информацией.
8. Дать определения терминов «Администратор автоматизированной системы (администратор АС)», «Администратор защиты», «Администратор базы данных». Различие и единство данных терминов**.**
9. Назовите основные направления мер защиты информации на основании ст.16. ФЗ «Об информации».
10. Права субъекта персональных данных – физического лица в соответствии с ФЗ «О Персональных данных»
11. Жизненный цикл автоматизированной системы (АС) в соответствии с ГОСТ 34.003-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы.
12. Дать определение терминов «Аутентичный документ», «Атрибут», в соответствии с ГОСТ 2.051-2006. Единая система конструкторской документации. Электронные документы. Общие положения
13. Идентичность данных в соответствии с ГОСТ Р 51170-98. Качество служебной информации.
14. Кодекс Российской Федерации об административных правонарушениях (КоАП РФ) в области правил защиты информации (ст. 13.11, 13.12, 13.13, 13.14, 17.13).
15. Уголовный кодекс РФ (УК РФ) о компьютерных преступлениях (ст.272)
16. УК РФ о компьютерных преступлениях (ст. 273)
17. УК РФ о компьютерных преступлениях (ст.274)
18. УК РФ о преступлениях, связанных с получением и разглашением информации, составляющей коммерческую, налоговую или банковскую тайну

7. Оценочные материалы 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 (или ее части)**	**Образовательные технологии**	**Этап освоения компетенции (или ее части)**
Информационная безопасность в системе национальной безопасности Российской Федерации.	ОК-3	Лекция, самостоятельная работа	Промежуточный
	ОК-4		Промежуточный
	ОК-7		Промежуточный

Наименование разделов, тем	Код формируемой компетенции (или ее части)	Образовательные технологии	Этап освоения компетенции (или ее части)
Национальные интересы Российской Федерации в информационной сфере и их обеспечение.	ПК-4		Промежуточный
Виды угроз информационной безопасности Российской Федерации. Источники угроз информационной безопасности	ОК-3	Лекция, самостоятельная работа	Промежуточный
	ОК-4		Промежуточный
	ОК-7		Промежуточный
	ПК-4		Промежуточный
Информационная безопасность и информационное противоборство.	ОК-3	Лекция, самостоятельная работа	Промежуточный
	ОК-4		Промежуточный
	ОК-7		Промежуточный
	ПК-4		Промежуточный
Обеспечение информационной безопасности объектов информатизационной сферы государства в условиях информационной войны.	ОК-3	Лекция, практическое занятие, самостоятельная работа	Промежуточный
	ОК-4		Промежуточный
	ОК-7		Промежуточный
	ПК-4		Промежуточный
Общие методы обеспечения информационной безопасности Российской Федерации.	ОК-3	Лекция, практическое занятие, самостоятельная работа, интерактивные образовательные технологии	Промежуточный
	ОК-4		Промежуточный
	ОК-7		Промежуточный
	ПК-4		Промежуточный
Законодательство РФ в области информационной безопасности. Правовой режим защиты государственной тайны. Правовые режимы защиты конфиденциальной информации	ОК-3	Лекция, самостоятельная работа, интерактивные образовательные технологии	Промежуточный
	ОК-4		Промежуточный
	ОК-7		Промежуточный
	ПК-4		Промежуточный
Лицензирование и сертификация в информационной сфере.	ОК-3	Лекция, самостоятельная работа	Промежуточный
	ОК-4		Промежуточный

Наименование разделов, тем	Код формируемой компетенции (или ее части)	Образовательные технологии	Этап освоения компетенции (или ее части)
Защита интеллектуальной собственности. Компьютерные правонарушения.	ОК-7		Промежуточный
	ПК-4		Промежуточный
Международное законодательство в области защиты информации. Организационное обеспечение	ОК-3	Самостоятельная работа	Промежуточный
	ОК-4		Промежуточный
	ОК-7		Промежуточный
	ПК-4		Промежуточный
Методы и средства обеспечения информационной безопасности компьютерных систем	ОК-3	Практическое занятие, самостоятельная работа	Промежуточный
	ОК-4		Промежуточный
	ОК-7		Промежуточный
	ПК-4		Промежуточный

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

№ п/п	Код компетенции (или ее части)	Уровни сформированности компетенции			Оценочные средства
		Пороговый (удовлетворительно)	Продвинутый (хорошо)	Высокий (отлично)	
1.	ОК-3	**Знать:** – способы сбора, передачи, хранения информации; – основные понятия и общеметодологические принципы теории информационной безопасности; – роль информационной безопасности в обеспечении национальной безопасности государства; – содержание основных понятий по	**Знать:** – способы сбора, передачи, хранения информации; – основные понятия и общеметодологические принципы теории информационной безопасности; – роль информационной безопасности в обеспечении национальной безопасности государства; – основные направления обеспечения	**Знать:** – способы сбора, передачи, хранения информации; – основные понятия и общеметодологические принципы теории информационной безопасности; – роль информационной безопасности в обеспечении национальной безопасности государства; – основные методы нарушения	Вопросы к зачету и /или бланковое тестирование

		правовому обеспечению информационной безопасности; – правовые способы защиты государственной тайны, конфиденциальной информации и интеллектуальной собственности; – основы правового регулирования взаимоотношений администрации и персонала в области защиты информации; **Уметь:** – подбирать и использовать соответствующие правовые, организационно-технические и экономические методы обеспечения информационной безопасности выбранных объектов; – разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов. **Владеть:** – навыками анализа	информационной безопасности объектов информационной сферы государства в условиях информационной войны; – содержание основных понятий по правовому обеспечению информационной безопасности; – правовые способы защиты государственной тайны, конфиденциальной информации и интеллектуальной собственности; – понятие и виды защищаемой информации, особенности государственной тайны как вида защищаемой информации; – основы правового регулирования взаимоотношений администрации и персонала в области защиты информации; **Уметь:** – подбирать и использовать соответствующие правовые, организационно-технические и экономические методы обеспечения информационной безопасности выбранных объектов;	конфиденциальности, целостности и доступности информации. – основные причины, виды, каналы утечки и искажения информации; – основные направления обеспечения информационной безопасности объектов информационной сферы государства в условиях информационной войны; – содержание основных понятий по правовому обеспечению информационной безопасности; – правовые способы защиты государственной тайны, конфиденциальной информации и интеллектуальной собственности; – понятие и виды защищаемой информации, особенности государственной тайны как вида защищаемой информации; – основы правового регулирования взаимоотношений администрации и персонала в области защиты информации; – правила лицензирования и	

		информационной инфраструктуры государства; – об информационном праве как основе информационного общества.	– применять действующую законодательную базу в области информационной безопасности; – разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов. **Владеть:** – навыками анализа информационной инфраструктуры государства; – навыками формальной постановки и решения задачи обеспечения информационной безопасности выбранного объекта телекоммуникационной системы;	сертификации в области защиты информации; – виды и признаки компьютерных преступлений, особенности основных следственных действий при расследовании указанных преступлений. **Уметь:** – подбирать и использовать соответствующие правовые, организационно-технические и экономические методы обеспечения информационной безопасности выбранных объектов; – отыскивать необходимые нормативные правовые акты и информационно-правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации; – применять действующую законодательную базу в области информационной безопасности; – разрабатывать проекты нормативных материалов, регламентирующи	

				х работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов. **Владеть:** – навыками анализа информационной инфраструктуры государства; – навыками формальной постановки и решения задачи обеспечения информационной безопасности выбранного объекта телекоммуникационной системы; – понятиями информационного права как основы информационного общества; – об информационном праве как основе информационного общества.	
2.	ОК-4	**Знать:** – способы сбора, передачи, хранения информации; – основные понятия и общеметодологические принципы теории информационной безопасности; – роль информационной	**Знать:** – способы сбора, передачи, хранения информации; – основные понятия и общеметодологические принципы теории информационной безопасности; – роль информационной	**Знать:** – способы сбора, передачи, хранения информации; – основные понятия и общеметодологические принципы теории информационной безопасности; – роль информационной	Вопросы к зачету и /или бланковое тестирование

		безопасности в обеспечении национальной безопасности государства; – содержание основных понятий по правовому обеспечению информационной безопасности; – правовые способы защиты государственной тайны, конфиденциальной информации и интеллектуальной собственности; – основы правового регулирования взаимоотношений администрации и персонала в области защиты информации; **Уметь:** – подбирать и использовать соответствующие правовые, организационно-технические и экономические методы обеспечения информационной безопасности выбранных объектов; – разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации, а также положений, инструкций и	безопасности в обеспечении национальной безопасности государства; – основные направления обеспечения информационной безопасности объектов информационной сферы государства в условиях информационной войны; – содержание основных понятий по правовому обеспечению информационной безопасности; – правовые способы защиты государственной тайны, конфиденциальной информации и интеллектуальной собственности; – понятие и виды защищаемой информации, особенности государственной тайны как вида защищаемой информации; – основы правового регулирования взаимоотношений администрации и персонала в области защиты информации; **Уметь:** – подбирать и использовать соответствующие правовые, организационно-	безопасности в обеспечении национальной безопасности государства; – основные методы нарушения конфиденциальности, целостности и доступности информации. – основные причины, виды, каналы утечки и искажения информации; – основные направления обеспечения информационной безопасности объектов информационной сферы государства в условиях информационной войны; – содержание основных понятий по правовому обеспечению информационной безопасности; – правовые способы защиты государственной тайны, конфиденциальной информации и интеллектуальной собственности; – понятие и виды защищаемой информации, особенности государственной тайны как вида защищаемой информации; – основы правового	

		других организационно-распорядительных документов. **Владеть:** – навыками анализа информационной инфраструктуры государства; – об информационном праве как основе информационного общества.	технические и экономические методы обеспечения информационной безопасности выбранных объектов; – применять действующую законодательную базу в области информационной безопасности; – разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов. **Владеть:** – навыками анализа информационной инфраструктуры государства; – навыками формальной постановки и решения задачи обеспечения информационной безопасности выбранного объекта телекоммуникационной системы;	регулирования взаимоотношений администрации и персонала в области защиты информации; – правила лицензирования и сертификации в области защиты информации; – виды и признаки компьютерных преступлений, особенности основных следственных действий при расследовании указанных преступлений. **Уметь:** – подбирать и использовать соответствующие правовые, организационно-технические и экономические методы обеспечения информационной безопасности выбранных объектов; – отыскивать необходимые нормативные правовые акты и информационно-правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации; – применять действующую законодательную	

				базу в области информационной безопасности; – разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов. **Владеть:** – навыками анализа информационной инфраструктуры государства; – навыками формальной постановки и решения задачи обеспечения информационной безопасности выбранного объекта телекоммуникационной системы; – понятиями информационного права как основы информационного общества; – об информационном праве как основе информационного общества.	
3.	ОК-7	**Знать:** – способы сбора, передачи, хранения информации; – основные	**Знать:** – способы сбора, передачи, хранения информации; – основные	**Знать:** – способы сбора, передачи, хранения информации; – основные	Вопросы к зачету и /или бланковое тестирование

		понятия и общеметодологические принципы теории информационной безопасности; – роль информационной безопасности в обеспечении национальной безопасности государства; – содержание основных понятий по правовому обеспечению информационной безопасности; – правовые способы защиты государственной тайны, конфиденциальной информации и интеллектуальной собственности; – основы правового регулирования взаимоотношений администрации и персонала в области защиты информации; **Уметь:** – подбирать и использовать соответствующие правовые, организационно-технические и экономические методы обеспечения информационной безопасности выбранных объектов; – разрабатывать проекты	понятия и общеметодологические принципы теории информационной безопасности; – роль информационной безопасности в обеспечении национальной безопасности государства; – основные направления обеспечения информационной безопасности объектов информационной сферы государства в условиях информационной войны; – содержание основных понятий по правовому обеспечению информационной безопасности; – правовые способы защиты государственной тайны, конфиденциальной информации и интеллектуальной собственности; – понятие и виды защищаемой информации, особенности государственной тайны как вида защищаемой информации; – основы правового регулирования взаимоотношений администрации и персонала в	понятия и общеметодологические принципы теории информационной безопасности; – роль информационной безопасности в обеспечении национальной безопасности государства; – основные методы нарушения конфиденциальности, целостности и доступности информации. – основные причины, виды, каналы утечки и искажения информации; – основные направления обеспечения информационной безопасности объектов информационной сферы государства в условиях информационной войны; – содержание основных понятий по правовому обеспечению информационной безопасности; – правовые способы защиты государственной тайны, конфиденциальной информации и интеллектуальной собственности; – понятие и виды защищаемой	

		нормативных материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов. **Владеть:** – навыками анализа информационной инфраструктуры государства; – об информационном праве как основе информационного общества.	области защиты информации; **Уметь:** – подбирать и использовать соответствующие правовые, организационно-технические и экономические методы обеспечения информационной безопасности выбранных объектов; – применять действующую законодательную базу в области информационной безопасности; – разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов. **Владеть:** – навыками анализа информационной инфраструктуры государства; – навыками формальной постановки и решения задачи обеспечения информационной безопасности выбранного объекта телекоммуникаци	информации, особенности государственной тайны как вида защищаемой информации; – основы правового регулирования взаимоотношений администрации и персонала в области защиты информации; – правила лицензирования и сертификации в области защиты информации; – виды и признаки компьютерных преступлений, особенности основных следственных действий при расследовании указанных преступлений. **Уметь:** – подбирать и использовать соответствующие правовые, организационно-технические и экономические методы обеспечения информационной безопасности выбранных объектов; – отыскивать необходимые нормативные правовые акты и информационно-правовые нормы в системе действующего	

			онной системы;	законодательства, в том числе с помощью систем правовой информации; – применять действующую законодательную базу в области информационной безопасности; – разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов. **Владеть:** – навыками анализа информационной инфраструктуры государства; – навыками формальной постановки и решения задачи обеспечения информационной безопасности выбранного объекта телекоммуникационной системы; – понятиями информационного права как основы информационного общества; – об информационном праве как основе информационного общества	

4.	ПК-3	**Знать:** – способы сбора, передачи, хранения информации; – основные понятия и общеметодологические принципы теории информационной безопасности; – роль информационной безопасности в обеспечении национальной безопасности государства; – содержание основных понятий по правовому обеспечению информационной безопасности; – правовые способы защиты государственной тайны, конфиденциальной информации и интеллектуальной собственности; – основы правового регулирования взаимоотношений администрации и персонала в области защиты информации; **Уметь:** – подбирать и использовать соответствующие правовые, организационно-технические и экономические методы обеспечения	**Знать:** – способы сбора, передачи, хранения информации; – основные понятия и общеметодологические принципы теории информационной безопасности; – роль информационной безопасности в обеспечении национальной безопасности государства; – основные направления обеспечения информационной безопасности объектов информационной сферы государства в условиях информационной войны; – содержание основных понятий по правовому обеспечению информационной безопасности; – правовые способы защиты государственной тайны, конфиденциальной информации и интеллектуальной собственности; – понятие и виды защищаемой информации, особенности государственной тайны как вида защищаемой информации;	**Знать:** – способы сбора, передачи, хранения информации; – основные понятия и общеметодологические принципы теории информационной безопасности; – роль информационной безопасности в обеспечении национальной безопасности государства; – основные методы нарушения конфиденциальности, целостности и доступности информации. – основные причины, виды, каналы утечки и искажения информации; – основные направления обеспечения информационной безопасности объектов информационной сферы государства в условиях информационной войны; – содержание основных понятий по правовому обеспечению информационной безопасности; – правовые способы защиты государственной тайны,	Вопросы к зачету и /или бланковое тестирование

		информационной безопасности выбранных объектов; – разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов. **Владеть:** – навыками анализа информационной инфраструктуры государства; – об информационном праве как основе информационного общества.	– основы правового регулирования взаимоотношений администрации и персонала в области защиты информации; **Уметь:** – подбирать и использовать соответствующие правовые, организационно-технические и экономические методы обеспечения информационной безопасности выбранных объектов; – применять действующую законодательную базу в области информационной безопасности; – разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов. **Владеть:** – навыками анализа информационной инфраструктуры государства; – навыками формальной постановки и решения задачи	конфиденциальной информации и интеллектуальной собственности; – понятие и виды защищаемой информации, особенности государственной тайны как вида защищаемой информации; – основы правового регулирования взаимоотношений администрации и персонала в области защиты информации; – правила лицензирования и сертификации в области защиты информации; – виды и признаки компьютерных преступлений, особенности основных следственных действий при расследовании указанных преступлений. **Уметь:** – подбирать и использовать соответствующие правовые, организационно-технические и экономические методы обеспечения информационной безопасности выбранных объектов; – отыскивать необходимые	

			обеспечения информационной безопасности выбранного объекта телекоммуникационной системы;	нормативные правовые акты и информационно-правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации; – применять действующую законодательную базу в области информационной безопасности; – разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов. **Владеть:** – навыками анализа информационной инфраструктуры государства; – навыками формальной постановки и решения задачи обеспечения информационной безопасности выбранного объекта телекоммуникационной системы; – понятиями информационного права как основы информационного	

				общества; – об информационном праве как основе информационного общества.	

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; – 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.	от 100 до 35% правильных ответов	**зачтено**
«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	от 75% до 50 % правильных ответов	**зачтено**

	освещении второстепенных вопросов, которые легко исправляются по замечанию преподавателя.		
«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 теоретического материала выявлена недостаточная сформированность компетенций, умений и навыков, студент не может применить теорию в новой ситуации; – продемонстрировано усвоение основной литературы.	от 50% до 35% правильных ответов	**зачтено**
«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
32. Структура информационной сферы и характеристика ее элементов.
33. Формирование информационных ресурсов и их квалификация.
34. Конституционные гарантии прав на информацию и механизм их реализации.
35. Понятие и структура информационной безопасности.
36. Информационная сфера и информационная среда.
37. Субъекты и объекты правоотношений в области информационной безопасности.
38. Понятие и виды защищаемой информации по законодательству РФ.
39. Отрасли законодательства, регламентирующие деятельность по защите информации.
40. Перспективы развития законодательства в области информационной безопасности.
41. Понятие правового режима защиты государственной тайны.
42. Государственная тайна как особый вид защищаемой информации и ее характерные признаки.
43. Реквизиты носителей сведений, составляющих государственную тайну.
44. Принципы, механизм и процедура отнесения сведений к государственной тайне, их засекречивания и рассекречивания.
45. Органы защиты государственной тайны и их компетенция.
46. Порядок допуска и доступа к государственной тайне.
47. Перечень и содержание организационных мер, направленных на защиту государственной тайны.
48. Система контроля за состоянием защиты государственной тайны.
49. Юридическая ответственность за нарушения правового режима защиты государственной тайны (уголовная, административная, дисциплинарная).
50. Конфиденциальная информация: персональные данные, служебная тайна, коммерческая тайна, банковская тайна, тайна следствия и судопроизводства, профессиональная тайна.
51. Правовые режимы конфиденциальной информации: содержание и особенности. Основные требования, предъявляемые к организации защиты конфиденциальной информации.

52. Юридическая ответственность за нарушения правового режима конфиденциальной информации (уголовная, административная, гражданско-правовая, дисциплинарная).
53. Правовая регламентация охранной деятельности.
54. Понятия лицензирования по российскому законодательству.
55. Виды деятельности в информационной сфере, подлежащие лицензированию.
56. Правовая регламентация лицензионной деятельности в области защиты информации.
57. Объекты лицензирования в сфере защиты информации.
58. Специальные экспертизы и государственная аттестация руководителей.
59. 28.Органы лицензирования и их полномочия.
60. 29.Контроль за соблюдением лицензиатами условий ведения деятельности.
61. Понятие сертификации по российскому законодательству.
62. Правовая регламентация сертификационной деятельности в области защиты информации.
63. Правовые основы защиты информации с использованием технических средств
64. Законодательство РФ об интеллектуальная собственности.
65. Понятие интеллектуальной собственности.
66. Объекты и субъекты авторского права.
67. Исключительные авторские права. Смежные права.
68. Правовая охрана программ для ЭВМ, баз данных и топологий интегральных микросхем.
69. Защита авторских и смежных прав. Основы патентных правоотношений.
70. Условия патентоспособности.
71. Объекты изобретения, связанные с электронно-вычислительной техникой и информационными технологиями. Авторы изобретений и патентообладатели.
72. .Механизм патентования.
73. Защита прав патентообладателей и авторов.
74. Особенности договорных отношений в области информационной безопасности.
75. Правовое регулирование взаимоотношений администрации и персонала в области обеспечения информационной безопасности. Особенности трудовых отношений.
76. Понятие оперативно-розыскной деятельности и оперативно-розыскных мероприятий по законодательству РФ.
77. Органы, уполномоченные на осуществление оперативно-розыскной деятельности.
78. Система правовых актов, регулирующих проведение оперативно- розыскных мероприятий.
79. Преступления в сфере компьютерной информации.
80. Признаки и элементы состава преступления. Криминалистическая характеристика компьютерных преступлений.
81. Расследование компьютерного преступления. Особенности основных следственных действий.
82. Экспертиза преступлений в области компьютерной информации.
83. Проблемы судебного преследования за преступления в сфере компьютерной информации.
84. Законодательство РФ об участии в международном информационном обмене.
85. Правовой режим участия в международном обмене.
86. Субъекты и объекты международного информационного обмена.
87. Национальные законодательства о компьютерных правонарушениях и защите информации.
88. Международное сотрудничество в области борьбы с компьютерной преступностью

Задания к зачету

Задание 1

Охарактеризуйте группы работ при проведении аудита информационной

безопасности информационной системы.

Задание 2
Охарактеризуйте подходы к построению системы информационной безопасности.

Задание 3
Создайте защищенный PDF файл

Задание 4
Создайте защищенный файл с помощью шифра AES

Типовые задания бланкового тестирования для промежуточной аттестации

Вариант 1.

Выберите верный ответ или ответы
1. Защищаемые государством сведения в области военной, внешнеполитической и внешнеэкономической деятельности, распространение которых может нанести ущерб безопасности РФ.
1. Государственная тайна
2. Коммерческая тайна
3. Банковская тайна
4. Конфиденциальная информация

2. Защищенность страны от нападения извне, шпионажа, покушения на государственный и общественный строй:
1. Информационная безопасность
2. Безопасность
3. Национальная безопасность
4. Защита информации

3. Какие степени секретности и грифы секретности носителей сведений, установлены законодательством РФ. Отметьте правильный вариант:
1. для служебного пользования
2. совершенно секретно
3. конфиденциально
4. особой важности
5. строго конфиденциально
6. секретно

4. Для обеспечения безопасности ИС применяют системы защиты информации, которые представляют собой комплекс
1. организационно-технологических мер, программно-технических средств и правовых норм
2. аппаратно-технических
3. административно-технических мер
4. администрирования, конфигурирования систем и средств защиты

5. Инцидент информационной безопасности это:
1. идентифицированное состояние системы, сервиса или сети, свидетельствующее о возможном нарушении политики безопасности или отсутствии механизмов защиты, либо прежде неизвестная ситуация, которая может иметь отношение к безопасности

2. одно или серия нежелательных или неожиданных событий информационной безопасности, имеющих значительную вероятность нарушения бизнес операций или представляющих угрозу для информационной безопасности
3. процесс сравнения оценочной величины риска с установленным критерием с целью определения уровня значимости риска
4. слабость одного или нескольких активов, которая может быть использована одной или несколькими угрозами

Запишите ответ на предложенный вопрос

6. Не подлежат отнесению к государственной тайне сведения…
_____

7. В соответствии с ФЗ «О государственной тайне» к числу основных принципов отнесения информации к государственной тайне относятся…
_____
8. Закон Российской Федерации «о государственной тайне» вступил в силу
_____
9. Отнесение сведений к государственной тайне и их засекречивание осуществляется в соответствии с принципами…
_____
10. Установление ограничений на распространение сведений момента их получения (разработки) или заблаговременно – это принцип…
_____

11. Соотнесите с буквами цифры, установив верные соотношения основных понятий в области информационной безопасности

А) Атака	1) некоторое неудачное свойство системы, которое делает возможным возникновение и реализацию угрозы
Б) Уязвимость АС	2) система со средствами защиты, которые успешно и эффективно противостоят угрозам безопасности
В) Угроза безопасности АС	3) возможные воздействия на АС, которые прямо или косвенно могут нанести ущерб ее безопасности
Г) Защищенная система	4) действие, предпринимаемое злоумышленником, которое заключается в поиске и использовании той или иной уязвимости системы

А	Б	В	Г

12. Соотнесите с буквами цифры, установив верные соотношения основных видов угроз для АС и их определений

А) Угроза нарушения конфиденциальности	1) Любое умышленное изменение информации, хранящейся в ВС или передаваемой от одной системы в другую
Б) Угроза отказа служб	2) Возникает всякий раз, когда в результате преднамеренных действий, предпринимаемых другим пользователем или злоумышленником, блокируется доступ к некоторому ресурсу АС
В) Угроза нарушения целостности	3) Заключается в том, что информация становится известной тому, кто не располагает полномочиями доступа к ней

А	Б	В

13. Соотнесите с буквами цифры, установив классификацию угроз по ряду признак

А) по природе возникновения	1) пассивные и активные
Б) по непосредственному источнику	2) направленные на использование прямого стандартного пути доступа к ресурсам и направленные на использование скрытого нестандартного доступа к ресурсам АС
В) по степени воздействия на АС	3) естественные или искусственные
Г) по способу доступа к ресурсам АС	4) природная среда, человек, санкционированные программные средства и несанкционированные программные средства

А	Б	В	Д

14. Соотнесите с буквами цифры, установив верные соотношения принципов информационной безопасности и их определений

А) Целостность данных	1) это свойство характеризует способность обеспечивать своевременный и беспрепятственный доступ полноправных пользователей к требуемой информации.
Б) Конфиденциальность	2) такое свойство, в соответствии с которым информация сохраняет свое содержание и структуру в процессе ее передачи и хранения. Создавать, уничтожать или изменять данные может только пользователь, имеющий право доступа.
В) Доступность информации	3) свойство, которое указывает на необходимость ограничения доступа к конкретной информации для обозначенного круга лиц. Таким образом, конфиденциальность дает гарантию того, что в процессе передачи данных, они могут быть известны только авторизованным пользователям
Г) Достоверность	4) данный принцип выражается в строгой принадлежности информации субъекту, который является ее источником или от которого она принята.

А	Б	В	Д

15. Соотнесите с буквами цифры, установив верные соотношения способов защиты информации и их определений

А) Маскировка	1) способы защиты информации, при которых осуществляется управление над всеми компонентами информационной системы.
Б) Управление	2) важнейший метод защиты информационных систем, предполагающий введение особых инструкций, согласно которым должны осуществляться все манипуляции с охраняемыми данными.
В) Регламентация	3) способы защиты информации, предусматривающие преобразование данных в форму, не пригодную для восприятия посторонними лицами. Для расшифровки требуется знание принципа.
Г) Принуждение	4) методы защиты информации, тесно связанные с регламентацией, предполагающие введение комплекса мер, при которых работники вынуждены выполнять установленные правила. Если используются

	способы воздействия на работников, при которых они выполняют инструкции по этическим и личностным соображениям, то речь идет о побуждении.

А	Б	В	Д

16. Расположить в хронологическом порядке этапы построения системы информационной безопасности в соответствии со стандартизованным жизненным циклом ИС: *внедрение и аттестация; аудит безопасности; создание служб и механизмов безопасности; техническая поддержка и сопровождение; проектирование системы проектирование архитектуры системы безопасности.*

1_____
2_____
3_____
4_____
5_____
6_____

17. Расположить в хронологическом порядке этапы трансформации идей информационной безопасности:

Этап	Характеристика
	обусловлен созданием и развитием локальных информационно-коммуникационных сетей
	связан с началом использования искусственно создаваемых технических средств электро- и радиосвязи
	характеризуется использованием естественно возникавших средств информационных коммуникаций
	связан с изобретением и внедрением в практическую деятельность электронно-вычислительных машин (компьютеров)
	связан с использованием сверхмобильных коммуникационных устройств с широким спектром задач
	связан с подготовкой и внедрением проекта международной концепции информационной безопасности
	связан с появлением радиолокационных и гидроакустических средств
	связан с созданием и развитием глобальных информационно-коммуникационных сетей с использованием космических средств обеспечения

18. Расположить по мере уменьшения значимости нормативные акты, которыми руководствуются при проведении аудита ИБ: *Отраслевые стандарты и рекомендации (СТО БР ИББС, NIST, NERC, PCI; DSS); Руководящие документы ФСБ и ФСТЭК; Законы РФ; Государственные стандарты РФ; Международные стандарты и рекомендации (ISO/IEC); Рекомендации (Best Practice) на основе мирового опыта; Нормативные акты и стандарты предприятия.*

1_____
2_____
3_____
4_____
5_____
6_____
7_____

19. Расположить в порядке увеличения объемов хранимой информации уровни реализации базы данных правовой информации: региональный, федеральный, муниципальный.
1_____
2_____
3_____
19. Расположить в порядке увеличения объемов хранимой информации уровни реализации базы данных правовой информации: региональный, федеральный, муниципальный.
1_____
2_____
3_____
Расположить в порядке классификации информационных систем персональных данных, определенной Постановлением Правительства Российской Федерации от 17 ноября 2007 г. № 781, категории персональных данных:

Категория	Характеристика
	ПД, позволяющие идентифицировать субъекта ПД и получить о нем дополнительную информацию, за исключением ПД, относящихся к категории 1
	обезличенные и (или) общедоступные персональные данные
	ПД, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;
	персональные данные, позволяющие идентифицировать субъекта ПД

Вариант 2.

Задание № 1
Вопрос:

Выберите несколько из 4 вариантов ответа:
1) не допустить подмены (модификации) элементов информации при сохранении ее целостности
2) не допустить несанкционированного получения информации лицами или процессами, не имеющими на это соответствующих полномочий
3) обеспечить ее физическую целостность, т.е. не допустить искажения или уничтожения элементов информации
4) быть уверенным в том, что передаваемые (продаваемые) владельцем информации ресурсы будут использоваться только в соответствии с обговоренными сторонами условиями

Задание № 2
Вопрос:
Документированная информация это

Выберите один из 3 вариантов ответа:
1) зафиксированная на материальном носителе информация вместе с реквизитами, позволяющими ее идентифицировать.
2) зафиксированная на материальном носителе информация
3) зафиксированная на материальном носителе информация без реквизитов, позволяющих ее идентифицировать.

Задание № 3

Вопрос:

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.

Выберите несколько из 4 вариантов ответа:

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

Задание № 4

Вопрос:

Государственная тайна - это принадлежащие государству (государственному учреждению) сведения о его военной, внешнеполитической, экономической, разведывательной, контрразведыватсльной 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:

Выберите несколько из 4 вариантов ответа:

1) "совершенно секретно"
2) "секретно"
3) "совсем секретно"
4) "особой важности"

Задание № 5

Вопрос:

Персональные данные - это

Выберите один из 3 вариантов ответа:

1) сведения о фактах, событиях и обстоятельствах в жизни гражданина, позволяющие идентифицировать его личность.
2) сведения о фактах, событиях и обстоятельствах в жизни гражданина, позволяющие идентифицировать и аутентифицировать компьютерную систему.
3) сведения о фактах, событиях и обстоятельствах в жизни гражданина, позволяющие идентифицировать компьютерную систему.

Задание № 6

Вопрос:

Сопоставьте определение и понятие

Укажите соответствие для всех 2 вариантов ответа:

1) 2) совокупность средств и методов сбора, обработки, передачи данных (первичной информации) для получения информации нового качества (информационного продукта) о состоянии объекта, процесса или явления

__ Информационная система (ИС)
__ Информационная технология (ИТ)

Задание № 7

Вопрос:

Информационное оружие от обычных средств поражения отличает:

Выберите несколько из 4 вариантов ответа:

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

Задание № 8

Вопрос:

Выберите один из 5 вариантов ответа:

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

Задание № 9

Вопрос:

В отсутствие строгого определения информация интуитивно рассматривается в широком смысле как

Выберите один из 2 вариантов ответа:

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

Задание № 10

Вопрос:

В методологии анализа информационной безопасности обычно выделяют следующие основные понятия:

Выберите несколько из 5 вариантов ответа:

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

Задание № 11

Вопрос:

Соотнесите наиболее важные свойства информации и определения

Укажите соответствие для всех 3 вариантов ответа:

1) это свойство, указывающее на необходимость введения ограничений доступа к данной информации для определенного круга лиц

2) это свойство, характеризующее способность обеспечивать своевременный и беспрепятственный доступ пользователей к необходимой информации
3) это свойство, заключающееся в существовании информации в неискаженном виде по отношению к некоторому фиксированному состоянию

__ Доступность
__ Целостность
__ Конфиденциальность

Задание № 12
Вопрос:
Классификация угроз информационной безопасности компьютерных систем может быть проведена по ряду базовых признаков. Сопоставьте признак и классификацию

Укажите соответствие для всех 4 вариантов ответа:
1) Природная среда. Человек. Санкционированные программно-аппаратные средства. Несанкционированные программно-аппаратные средства.
2) Естественные угрозы. Искусственные угрозы
3) Вне контролируемой зоны, территории (помещения). В пределах контролируемой зоны
4) Случайные угрозы. Преднамеренные угрозы.

__ По положению источника угроз
__ По природе возникновения
__ По степени преднамеренности проявления
__ По непосредственному источнику угроз

Задание № 13
Вопрос:
Сопоставьте определение и понятие

Укажите соответствие для всех 4 вариантов ответа:
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.
2) предоставление субъекту прав на доступ к объекту.
3) процесс распознавания элемента системы, обычно с помощью заранее определенного идентификатора или другой уникальной информации; каждый субъект или объект системы должен быть однозначно идентифицируем.
4) ограничение возможностей использования ресурсов системы программами, процессами или другими системами (для сети) в соответствии с правилами разграничения доступа.

__ Контроль доступа - это
__ Идентификация - это
__ Аутентификация - это
__ Авторизация - это

Задание № 14
Вопрос:
Сопоставьте определение и принципы информационной безопасности

Укажите соответствие для всех 6 вариантов ответа:
1) Суть этого принципа состоит в том, что защита информации не должна обеспечиваться только за счёт секретности структурной и функциональной организации системы защиты.
2) Предполагает необходимость учёта всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов
3) Часто приходится создавать системы защиты в условиях большой неопределённости. Принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечить 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
5) Предполагающий принятие соответствующих мер на всех этапах жизненного цикла КС (начиная с самых ранних стадий проектирования, а не только на этапе её эксплуатации)
6) Механизмы защиты должны быть интуитивно понятны и просты в использовании. Защита будет тем эффективнее, чем легче пользователю с ней работать.

__ Принцип простоты применения средств защиты
__ Открытость алгоритмов и механизмов защиты
__ Принцип непрерывности защиты
__ Принцип системности
__ Гибкость системы защиты
__ Принцип комплексности

Задание № 15
Вопрос:
Сопоставьте определение и понятие

Укажите соответствие для всех 2 вариантов ответа:
1) интегральная характеристика, выражающая свойства защищённости компьютерной системы в терминах, представляющих эту систему.
2) официально принятая система взглядов на проблему информационной безопасности на уровне государства, отрасли или отдельной организации

__ При этом под концепцией информационной безопасности понимается
__ Политика безопасности - это

Задание № 16
Вопрос:
С любым объектом информационной безопасности естественным образом связано существование той или иной угрозы, под которой понимается

Выберите один из 3 вариантов ответа:
1) 2) негативное воздействие на объект информационной безопасности, возникающее в процессе взаимодействия данного объекта с другими объектами или составляющих его компонентов между собой
3) 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.

Задание № 17

Вопрос:

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

Укажите соответствие для всех 5 вариантов ответа:

1) Является многоаспектным понятием, включающим как международные, так и национальные правовые нормы

2) Суть защиты заключается в приведении (преобразовании) информации к неявному виду с помощью специальных алгоритмов либо аппаратных средств и соответствующих кодовых ключей.

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

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.

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

__ Организационная защита информации
__ Программно-аппаратная защита информации
__ Инженерно-техническая защита информации

__ Правовая защита информации
__ Криптографическая защита информации

Задание № 18

Вопрос:

Расположить в порядке увеличения объемов хранимой информации уровни реализации базы данных правовой информации:

- региональный,
- федеральный,
- муниципальный.

Задание № 19

Вопрос:

Расположить в хронологическом порядке этапы построения системы информационной безопасности в соответствии со стандартизованным жизненным циклом ИС: *внедрение и аттестация; аудит безопасности;*

создание служб и механизмов безопасности; техническая поддержка и сопровождение; проектирование системы проектирование архитектуры системы безопасности.

Задание № 20

Вопрос:

Расположить в хронологическом порядке этапы трансформации идей информационной безопасности:

Этап	Характеристика
	обусловлен созданием и развитием локальных информационно-коммуникационных сетей
	связан с началом использования искусственно создаваемых технических средств электро- и радиосвязи
	характеризуется использованием естественно возникавших средств информационных коммуникаций
	связан с изобретением и внедрением в практическую деятельность электронно-вычислительных машин (компьютеров)
	связан с использованием сверхмобильных коммуникационных устройств с широким спектром задач
	связан с подготовкой и внедрением проекта международной концепции информационной безопасности
	связан с появлением радиолокационных и гидроакустических средств
	связан с созданием и развитием глобальных информационно-коммуникационных сетей с использованием космических средств обеспечения

Кейс-задания

Кейс-задание 1

Охарактеризуйте группы работ при проведении аудита информационной безопасности информационной системы.

Кейс-задание 2

Охарактеризуйте подходы к построению системы информационной безопасности.

Кейс-задание 3

Создайте защищенный PDF файл

Кейс-задание 4

Создайте защищенный файл с помощью шифра AES

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 основным формам текущего контроля (текущей аттестации) можно отнести контрольный опрос, письменные тестовые задания, разбор конкретных ситуаций, решение кейс-заданий, ситуационных задач, дискуссии, собеседование, рефераты, доклады, деловые и ролевые игры, компьютерные симуляции и т.д.

Промежуточная аттестация, как правило, осуществляется в конце семестра и может завершать изучение, как отдельной дисциплины, так и ее раздела (разделов)/модуля

(модулей). Промежуточная аттестация позволяет оценить совокупность знаний, умений и навыков, уровень сформированности компетенций (или их частей).

Основные формы промежуточной аттестации: экзамен

Промежуточная аттестация проводится в форме бланкового тестирования или в форме устного ответа на вопросы билета. Тестовое задание состоит из 20 вопросов и 2 практических заданий. Для проверки знаний используются вопросы и задания в закрытой форме, открытой форме, на определение правильной последовательности, на определение соответствия. Уровень сформированности компетенций (или их частей) проверяется с помощью практических заданий (ситуационных, производственных задач, кейс-заданий).

Билет по структуре состоит из 3 вопросов: 2 теоретических вопросов и одного практического задания. Вопросы формируются по темам (модулям) учебной дисциплины, практическое задание направлено на определение уровня освоения обучающимися компетенций.

Оценивание знаний, умений, навыков и (или) опыта деятельности носит 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 объективных оценочных средств. Формат оценочных материалов позволяет определить качество освоения обучающимися основных элементов содержания дисциплины и уровень сформированности компетенций (или их частей). 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»;
- 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, разделы (темы) дисциплины	Код контролируемой компетенции (или её части)	Оценочные средства		Способ контроля
			текущий контроль по дисциплине	промежуточная аттестация по дисциплине	
1	Информационная безопасность в системе национальной безопасности Российской Федерации. Национальные интересы Российской Федерации в информационной сфере и их обеспечение.	ОК-3, ОК-4, ОК-7, ПК-3	Задачи для самостоятельной работы, вопросы для самостоятельного изучения, рефераты	Вопросы и задания к зачету и (или) бланковое тестирование	Устно, письменно
2	Виды угроз информационной	ОК-3, ОК-4, ОК-7, ПК-3	Задачи для самостоятельной	Вопросы и задания к	Устно, письменно

	безопасности Российской Федерации. Источники угроз информационной безопасности.		работы, вопросы для самостоятельного изучения, рефераты	зачету и (или) бланковое тестирование	
3	Информационная безопасность и информационное противоборство.	ОК-3, ОК-4, ОК-7, ПК-3	Задачи для самостоятельной работы, вопросы для самостоятельного изучения, рефераты	Вопросы и задания к зачету и (или) бланковое тестирование	Устно, письменно
4	Обеспечение информационной безопасности объектов информатизационной сферы государства в условиях информационной войны.	ОК-3, ОК-4, ОК-7, ПК-3	Устный опрос, доклады, практические работы, тестовое задание, задачи для самостоятельной работы, вопросы для самостоятельного изучения, рефераты	Вопросы и задания к зачету и (или) бланковое тестирование	Устно, письменно
5	Общие методы обеспечения информационной безопасности Российской Федерации.	ОК-3, ОК-4, ОК-7, ПК-3	Устный опрос, доклады, практические работы, тестовое задание, презентация, задачи для самостоятельной работы, вопросы для самостоятельного изучения, рефераты	Вопросы и задания к зачету и (или) бланковое тестирование	Устно, письменно
6	Законодательство РФ в области информационной безопасности. Правовой режим защиты государственной тайны. Правовые режимы защиты конфиденциальной информации.	ОК-3, ОК-4, ОК-7, ПК-3	Задачи для самостоятельной работы, вопросы для самостоятельного изучения, рефераты	Вопросы и задания к зачету и (или) бланковое тестирование	Устно, письменно

7	Лицензирование и сертификация в информационной сфере. Защита интеллектуальной собственности. Компьютерные правонарушения.	ОК-3, ОК-4, ОК-7, ПК-3	Задачи для самостоятельной работы, вопросы для самостоятельного изучения, рефераты	Вопросы и задания к зачету и (или) бланковое тестирование	Устно, письменно
8	Международное законодательство в области защиты информации. Организационное обеспечение.	ОК-3, ОК-4, ОК-7, ПК-3	Задачи для самостоятельной работы, вопросы для самостоятельного изучения, рефераты	Вопросы и задания к зачету и (или) бланковое тестирование	Устно, письменно
9	Методы и средства обеспечения информационной безопасности компьютерных систем	ОК-3, ОК-4, ОК-7, ПК-3	Устный опрос, доклады, презентация, задачи для самостоятельной работы, вопросы для самостоятельного изучения, рефераты	Вопросы и задания к зачету и (или) бланковое тестирование	Устно, письменно

8. Основная и дополнительная литература, необходимая для освоения дисциплины

8.1 Основная литература

1. Основы информационной безопасности [Электронный ресурс] : учебник / В.Ю. Рогозин [и др.]. — Электрон. текстовые данные. — М. : ЮНИТИ-ДАНА, 2017. — 287 c. — 978-5-238-02857-6. — Режим доступа: http://www.iprbookshop.ru/72444.html .

8.2 Дополнительная литература

1. Галатенко В.А. Основы информационной безопасности [Электронный ресурс]/ Галатенко В.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 266 с.— Режим доступа: http://www.iprbookshop.ru/22424 .— ЭБС «IPRbooks», по паролю.

2. Морозов А.В. Информационное право и информационная безопасность. Часть 1 [Электронный ресурс] : учебник для магистров и аспирантов / А.В. Морозов, Л.В. Филатова, Т.А. Полякова. — Электрон. текстовые данные. — Москва, Саратов: Всероссийский государственный университет юстиции (РПА Минюста России), Ай Пи Эр Медиа, 2016. — 436 c. — 978-5-00094-296-3. — Режим доступа: http://www.iprbookshop.ru/72395.html .

3. Морозов А.В. Информационное право и информационная безопасность. Часть 2 [Электронный ресурс] : учебник для магистров и аспирантов / А.В. Морозов, Л.В. Филатова, Т.А. Полякова. — Электрон. текстовые данные. — Москва, Саратов: Всероссийский государственный университет юстиции (РПА Минюста России), Ай Пи Эр Медиа, 2016. — 604 c. — 978-5-00094-297-0. — Режим доступа: http://www.iprbookshop.ru/66771.html .

8.3 Нормативные правовые акты

1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [Электронный ресурс] / Доступ из справочно-правовой системы Консультант-Плюс.
2. Закон РФ от 21.07.1993 N 5485-1 «О государственной тайне» [Электронный ресурс] / Доступ из справочно-правовой системы Консультант-Плюс.
3. Федеральный закон от 13.01.1995 № 7-ФЗ «О порядке освещения деятельности органов государственной власти в государственных средствах массовой информации» [Электронный ресурс] / Доступ из справочно-правовой системы Консультант-Плюс.
4. Федеральный закон от 9.02.2009 г. № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» [Электронный ресурс] / Доступ из справочно-правовой системы Консультант-Плюс.
5. Закон Российской Федерации от 27.12.1991 г. № 2124-1 «О средствах массовой информации» [Электронный ресурс] / Доступ из справочно-правовой системы Консультант-Плюс.
6. Федеральный закон Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных» [Электронный ресурс] / Доступ из справочно-правовой системы Консультант-Плюс.
7. Постановление Правительства РФ от 14 ноября 2015 г. № 1235 «О федеральной государственной информационной системе координации информатизации» [Электронный ресурс] / Доступ из справочно-правовой системы Консультант-Плюс.
8. Постановление Правительства РФ от 30.06.2018 № 772 «Об определении состава сведений, размещаемых в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных» [Электронный ресурс] / Доступ из справочно-правовой системы Консультант-Плюс.
9. Постановление Правительства РФ от 23.12.2015 № 1414 «О порядке функционирования единой информационной системы в сфере закупок» [Электронный ресурс] / Доступ из справочно-правовой системы Консультант-Плюс.
10. Федеральный закон от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи» [Электронный ресурс] / Доступ из справочно-правовой системы Консультант-Плюс.
11. Постановление Правительства РФ от 25.08.2012 № 852 «Об утверждении Правил использования усиленной квалифицированной электронной подписи при обращении за получением государственных и муниципальных услуг и о внесении изменения в Правила разработки» [Электронный ресурс] / Доступ из справочно-правовой системы Консультант-Плюс.

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

1. .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)
2. http://www.infosecurity.report.ru (портал по информационной безопасности)
3. .http://www.void.ru/ (портал по информационной безопасности)
4. http://www.infosec.ru (Сервер компании НИП «Информзащита»)
5. http://www.jetinfo.ru/ (Информационный бюллетень «Jet Info» с тематическим разделом по информационной безопасности)

6. http://pdfcreator.ru/ (Официальный сайт программы PDFCreator)
7. http://en.protectorion.com/ (Официальный сайт программы Protectorion ToGo)
8. http://www.piriform.com/recuva (Официальный сайт программы Recuva)
9. http://www.handyrecovery.ru/ (Официальный сайт программы Handy Recovery)
10. http://www.pandorarecovery.com/local/ru/ (Официальный сайт программы Pandora Recovery)
11. http://www.drweb.ru/ (Официальный сайт программы Dr.Web)
12. http://www.consultant.ru/ (Официальный сайт компании «Консультант Плюс»)

10. Методические указания для обучающихся по освоению дисциплины

Методические указания для лекционных занятий

Работа на лекции является очень важным видом студенческой деятельности для изучения дисциплины «Организационно-правовые основы информационной безопасности». 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 студента 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 студентов по контрольным вопросам семинарского занятия.

Выступление на семинаре должно быть компактным и вразумительным, без неоправданных отступлений и рассуждений. Студент 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 студенту следует повторить выводы, сконструированные на семинаре, проследив логику их построения, отметив положения, лежащие в их основе. Для этого студенту в течение семинара следует делать пометки. Более того в случае неточностей и (или) непонимания какого-либо вопроса пройденного материала студенту 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 студентов; 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 студентов.

Формы и виды самостоятельной работы студентов: 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 студентов, 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 студентов 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 студентов преподаватель, ведущий семинарские занятия. Тестирование ставит целью оценить уровень освоения студентами дисциплины в целом, либо её отдельных тем, а также знаний и умений, предусмотренных компетенциями. Тестирование проводится для

студентов 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 студент 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 студента 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 студенту, по окончании представления доклада, могут быть заданы вопросы по теме доклада. Рекомендуемый объем 3-5 страниц компьютерного (машинописного) текста. К докладу студент 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 студента 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 студенты.

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 студента. Специфической задачей студента 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 студент 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 студент вновь обращается к уже изученному (пройденному) учебному материалу.

Подготовка студента 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 «Организационно-правовые основы информационной безопасности» студенты 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 студентом; семинарские занятия способствуют получению более высокого уровня знаний; 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 в системе национальной безопасности Российской Федерации. Национальные интересы Российской Федерации в информационной сфере и их обеспечение.	
2	Виды угроз информационной безопасности Российской Федерации. Источники угроз информационной безопасности.	
3	Информационная безопасность и информационное противоборство.	
4	Обеспечение информационной безопасности объектов информатизационной сферы государства в условиях информационной войны.	
5	Общие методы обеспечения информационной безопасности Российской Федерации.	Презентация «Методология защиты информации»
6	Законодательство РФ в области информационной безопасности. Правовой режим защиты государственной тайны. Правовые	Презентация «Правовой режим защиты государственной тайны» Презентация «Законодательные акты технической защиты информации»

	режимы защиты конфиденциальной информации.	
7	Лицензирование и сертификация в информационной сфере. Защита интеллектуальной собственности. Компьютерные правонарушения.	
8	Международное законодательство в области защиты информации. Организационное обеспечение.	
9	Основы комплексного обеспечения информационной безопасности. Методы и средства обеспечения информационной безопасности компьютерных систем	

11.2 Перечень лицензионного программного обеспечения

1. MicrosoftWindows7 Starter предустановленная лицензионная;
2. Microsoft Office Professional Plus 2007 Russian Academik OPEN No Level; Лицензия № 42859743, Лицензия № 42117365;
3. Microsoft Office Professional Plus 2007 Russian Academik OPEN No Level; Лицензия № 42859743

11.3 Современные профессиональные базы данных

1. Универсальная интернет-энциклопедия Wikipedia http://ru.wikipedia.org
2. Университетская библиотека Онлайн http://www.biblioclub.ru
3. Сервис полнотекстового поиска по книгам http://books.google.ru
4. Научная электронная библиотека eLIBRARY.RU http://elibrary.ru
5. Федеральный образовательный портал «Российское образование» http://www.edu.ru

11.4 Информационные справочные системы, используемые при осуществлении образовательного процесса

1. Справочная правовая система Консультант Плюс- договор №21/2018/К/Пр от 09.01.2018

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

Учебные занятия по дисциплине «Организационно-правовые основы информационной безопасности» проводятся в учебных кабинетах, оснащенных соответствующим оборудованием и программным обеспечением:

№ п/п	№ учебной аудитории	Наименование оборудования	Наименование оборудованных учебных кабинетов, объектов для проведения практических занятий
1	2	3	4
1.	305009, г. Курск, ул. Интернациональная, д.6-б. Учебная аудитория № 13 для проведения занятий семинарского	Рабочие места студентов: стулья, парты. Рабочее место преподавателя: стол, стул, аудиторная меловая доска, проектор Epson LCD	Справочная правовая система Консультант Плюс - договор №21/2018/К/Пр от 09.01.2018; Microsoft Windows Vista Business Russian Upgrade Academik OPEN No Level; Лицензия № 42859743, Лицензия № 42117365; Microsoft Office Professional Plus 2007

	типа, выполнения курсовых работ, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, помещение для хранения и профилактического обслуживания учебного оборудования, лаборатория «Информационные технологии в управлении».	Projector, экран для проектора. Наборы демонстрационного оборудования и учебно-наглядных пособий, информационные стенды: «Проектирование, создание и работа с базами данных», «Технология хранения, поиска и сортировки информации», «Программное обеспечение ПК(ЭВМ) по ПК(ЭВМ)». Монитор LCD Monitor 17” Acer AL1716Fs- 10 шт. Компьютер Intel Pentium Dual CPU E2140- 10 шт. Клавиатура –10 шт. Мышь- 10 шт. Имеется локальная сеть. Имеется доступ в Интернет на всех ПК.	Russian Academik OPEN No Level; Лицензия № 42859743, Лицензия № 42117365; Microsoft Office Professional Plus 2007 Russian Academik OPEN No Level; Лицензия № 42859743.
2.	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.	Справочная правовая система Консультант Плюс- договор №21/2018/К/Пр от 09.01.2018; Microsoft Windows 7 Starter предустановленная лицензионная; Microsoft Office Professional Plus 2007 Russian Academik OPEN No Level; Лицензия № 42859743, Лицензия № 42117365; Microsoft Office Professional Plus 2007 Russian Academik OPEN No Level; Лицензия № 42859743.

13. Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

При обучении лиц с ограниченными возможностями здоровья учитываются их индивидуальные психофизические особенности. Обучение инвалидов осуществляется также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).

Для лиц с нарушением слуха возможно предоставление учебной информации в визуальной форме (краткий конспект лекций; тексты заданий, напечатанные увеличенным шрифтом), на аудиторных занятиях допускается присутствие ассистента, а также сурдопереводчиков и тифлосурдопереводчиков. Текущий контроль успеваемости осуществляется в письменной форме: обучающийся письменно отвечает на вопросы, письменно выполняет практические задания. Доклад (реферат) также может быть представлен в письменной форме, при этом требования к содержанию остаются теми же, а требования к качеству изложения материала (понятность, качество речи, взаимодействие с аудиторией и т. д.) заменяются на соответствующие требования, предъявляемые к письменным работам (качество оформления текста и списка литературы, грамотность, наличие иллюстрационных материалов и т.д.). Промежуточная аттестация для лиц с нарушениями слуха проводится в письменной форме, при этом используются общие критерии оценивания. При необходимости время подготовки к ответу может быть увеличено.

Для лиц с нарушением зрения допускается аудиальное предоставление информации, а также использование на аудиторных занятиях звукозаписывающих устройств (диктофонов и т.д.). Допускается присутствие на занятиях ассистента (помощника), оказывающего обучающимся необходимую техническую помощь. Текущий контроль успеваемости осуществляется в устной форме. При проведении промежуточной аттестации для лиц с нарушением зрения тестирование может быть заменено на устное собеседование по вопросам.

Для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, на аудиторных занятиях, а также при проведении процедур текущего контроля успеваемости и промежуточной аттестации могут быть предоставлены необходимые технические средства (персональный компьютер, ноутбук или другой гаджет); допускается присутствие ассистента (ассистентов), оказывающего обучающимся необходимую техническую помощь (занять рабочее место, передвигаться по аудитории, прочитать задание, оформить ответ, общаться с преподавателем).