МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
САМАРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПУТЕЙ СООБЩЕНИЯ

Приложение 2
к рабочей программе дисциплины

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Информационная безопасность

(наименование дисциплины(модуля)

Направление подготовки / специальность

27.03.05 Инноватика

(код и наименование)

Направленность (профиль)/специализация

Управление инновациями на транспорте

(наименование)

Содержание

1. Пояснительная записка.
2. Типовые контрольные задания или иные материалы для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих уровень сформированности компетенций.
3. Методические материалы, определяющие процедуру и критерии оценивания сформированности компетенций при проведении промежуточной аттестации.

1. Пояснительная записка

Цель промежуточной аттестации – оценивание промежуточных и окончательных результатов обучения по дисциплине, обеспечивающих достижение планируемых результатов освоения образовательной программы.

Перечень компетенций, формируемых в процессе освоения дисциплины

Код и наименование компетенции	Код индикатора достижения компетенции
ОПК-5 Способен решать задачи в области инновационных процессов в науке, технике и технологии с учетом нормативно-правового регулирования в сфере интеллектуальной собственности	**ОПК-5.1:** Оформляет техническую документацию при выполнении задач профессиональной деятельности согласно стандартам
ОПК-3 Способен использовать фундаментальные знания для решения базовых задач управления в технических системах с целью совершенствования в профессиональной деятельности	**ОПК-3.3 :** Составляет обзоры, аннотации, рефераты, научные доклады, публикации и библиографии по научно-исследовательской работе с учетом требований информационной безопасности

Результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Оценочные материалы
ОПК-5.1: Оформляет техническую документацию при выполнении задач профессиональной деятельности согласно стандартам	**Обучающийся знает:** Основные методы и средства защиты конфиденциальной информации; состав и организацию систем информационной безопасности, методы криптографических преобразований; основные стандарты и протоколыь шифрования и электронной подписи; методы и средства обеспечения информационной безопасности компьютерных систем; современные методы обеспечения целостности и защиты информации и программных средств от несанкционированного доступа и копирования; современные подходы к построению систем защиты информации.	Вопросы тестирования № 1-10

	Обучающийся умеет: определять и анализировать угрозы безопасности информации в зависимости от среды эксплуатации продуктов информационных технологий; использовать современные программные средства для защиты информации; принимать адекватные решения при выборе средств защиты информации на основе анализа угроз; разрабатывать и создавать типовые схемы защиты информации на основе современных средств обеспечения информационной безопасности; обоснованно выбирать соответствующие организационные и программно-аппаратные средства для организации систем информационной защиты.	Задания №(1-3)
	Обучающийся владеет: навыками разработки защищенных приложений; навыками создания защищенной среды с помощью аппаратно-программных средств защиты; навыками самостоятельного проектирования систем защиты информации; методами оценки эффективности систем защиты информации в компьютерных системах.	Задания № (6-8)
ОПК-3.3 : Составляет обзоры, аннотации, рефераты, научные доклады, публикации и библиографии по научно-исследовательской работе с учетом требований информационной безопасности	**Обучающийся знает:** информационно-коммуникационные технологии и с учетом основных требований информационной безопасности.	Вопросы тестирования № 11-20
	Обучающийся умеет: решать сложные поставленные задачи, применяя принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности, подготавливать обзоры, аннотации.	Задания № (4-5)
	Обучающийся владеет: навыками составления рефератов, научные докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.	Задания № (9-10)

Промежуточная аттестация (экзамен) проводится в одной из следующих форм:

1) проводиться в форме устного ответа на вопросы из перечня
2) выполнение заданий в ЭИОС СамГУПС.

2. Типовые[1] контрольные задания или иные материалы для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих уровень сформированности компетенций

2.1 Типовые вопросы (тестовые задания) для оценки знаниевого образовательного результата

Проверяемый образовательный результат:

Код и наименование индикатора достижения компетенции	Образовательный результат
ОПК-5.1: Оформляет техническую документацию при выполнении задач профессиональной деятельности согласно стандартам	**Обучающийся знает:** основные методы и средства защиты конфиденциальной информации; состав и организацию систем информационной безопасности, методы криптографических преобразований; основные стандарты и протоколы шифрования и электронной подписи; методы и средства обеспечения информационной безопасности компьютерных систем; современные методы обеспечения целостности и защиты информации и программных средств от несанкционированного доступа и копирования; современные подходы к построению систем защиты информации.

Примеры вопросов/заданий

1. При количественном подходе риск измеряется в терминах
денежных потерь
заданных с помощью шкалы
заданных с помощью ранжирования
объема информации

2. Присвоение субъектам и объектам доступа уникального номера, шифра, кода и т.п. с целью получения доступа к информации – это
идентификация
аудит
авторизация
аутентификация

3. Программная закладка внедряется в ПЗУ, системное или прикладное программное обеспечение и сохраняет всю или выбранную информацию в скрытой области памяти в модели воздействия
перехват
компрометация
наблюдение
уборка мусора

4. Процесс определения риска, применения средств защиты для сокращения риска с последующим определением приемлемости остаточного риска, называется
управлением риском
мониторингом средств защиты
оптимизацией средств защиты
минимизацией риска

5. С помощью открытого ключа информация
зашифровывается
копируется
транслируется
расшифровывается

6. Согласно «Европейским критериям» для систем с высокими потребностями в обеспечении целостности предназначен класс
F-IN
F-DX
F-DI
F-AV

7. Согласно «Европейским критериям» на распределенные системы обработки информации ориентирован класс
F-DI

F-IN
F-AV
F-DX

8. Согласно «Оранжевой книге» с объектами должны быть ассоциированы

метки безопасности
электронные подписи
типы операций
уровни доступа

9. Содержанием параметра угрозы безопасности информации «конфиденциальность» является

несанкционированное получение уничтожение
искажение
несанкционированная модификация

10. Гарантия сохранности данными правильных значений, которая обеспечивается запретом для неавторизованных пользователей каким-либо образом модифицировать, разрушать или создавать данные – это

целостность
детерминированность
восстанавливаемость
доступность

ОПК-3.3 : Составляет обзоры, аннотации, рефераты, научные доклады, публикации и библиографии по научно-исследовательской работе с учетом требований информационной безопасности	**Обучающийся знает:** информационно-коммуникационные технологии и с учетом основных требований информационной безопасности.

Примеры вопросов/заданий

11. Меры каких уровней необходимо принимать при обеспечении защиты интересов субъектов информационных отношений?

1) социального;
2) законодательного;
3) исполнительного;
4) административного;
5) экономического;
6) процедурного;
7) функционального;
8) программно-технического;
9) программно-аппаратного.

1**2. Что относится к основным составляющим информационной безопасности (выберите несколько вариантов ответа)?**

1) защита информации;
2) компьютерная безопасность;
3) экологическая безопасность;
4) защищенность информации и поддерживающей инфраструктуры;
5) защита от информации;
6) защищенность потребностей граждан.

1**3. Что относится к первоочередным задачам защиты информации (выберите несколько вариантов ответа)?**

1) обеспечение качества информационных ресурсов;
2) обеспечение целостности информационных ресурсов;
3) обеспечение доступности информационных ресурсов;
4) обеспечение надежности информационных ресурсов;
5) обеспечение конфиденциальности информационных ресурсов.

1**4. Обозначьте основные направления деятельности на законодатель- ном уроне в сфере обеспечения информационной безопасности (выберите несколько вариантов ответа)?**

1) разработка новых законов с учетом интересов всех категорий субъектов информационных отношений;

2) ориентация на созидательные законы;
3) ориентация на карательные законы;
4) создание уникальных стандартов и сертификационных нормативов, актуальных только в России;
5) интеграция в мировое правовое пространство;
6) учет современного состояния информационных технологий;
7) использование исключительно собственного опыта при создании нормативно-правовой базы в области информационной безопасности.

15. Выделите основные группы процедурных мер, направленных на обеспечение информационной безопасности (выберите несколько вариантов ответа).

1) программная защита;
2) управление персоналом;
3) управление ресурсами;
4) аппаратная защита;
5) физическая защита;
6) поддержание работоспособности;
7) реагирование на нарушения режима безопасности;
8) обеспечение стабильности;
9) планирование восстановительных работ.

16. На чем основывается политика информационной безопасности в организации?

1) на выявлении всех возможных угроз информационной безопасности организации;
2) на поиске уязвимостей информационной системы организации;
3) на анализе рисков, признанных реальными для информационной системы организации;
4) на закупке оборудования, предотвращающего утечку информации по техническим каналам;
5) на регистрации всех действий персонала при работе с защищаемой информацией.

17. Уполномоченными лицами считаются … (выберите несколько вариантов ответа)

1) собственники информации;
2) владельцы информации;
3) пользователи информации;
4) пользователи, получившие право работы с информацией от ее владельца;
5) государственные служащие;
6) работники силовых структур.

18. Уязвимость — это …

1) наличие узких мест в системе защиты информации;
2) слабость системы информационной безопасности;
3) незащищенность или ошибка в объекте, которая может привести к возникновению угрозы;
4) наличие угроз информационной безопасности;
5) незащищенность объектов информационной системы.

19. Неумышленное происшествие с деструктивным воздействием на объект — это …

1) ошибка;
2) катастрофа;
3) авария;
4) повреждение;
5) поломка.

20. Что понимается под совокупностью документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов?

1) информационная политика;
2) безопасность информации;
3) политика безопасности;
4) регламентация доступа;
5) организация защиты.

[1] Приводятся типовые вопросы и задания. Оценочные средства, предназначенные для проведения аттестационного мероприятия, хранятся на кафедре в достаточном для проведения оценочных процедур количестве вариантов. Оценочные средства подлежат актуализации с учетом развития науки, образования, культуры, экономики, техники,технологий и социальной сферы. Ответственность за нераспространение содержания оценочных средств среди обучающихся университета несут заведующий кафедрой и преподаватель – разработчик оценочных средств.

2.2 Типовые задания для оценки навыкового образовательного результата

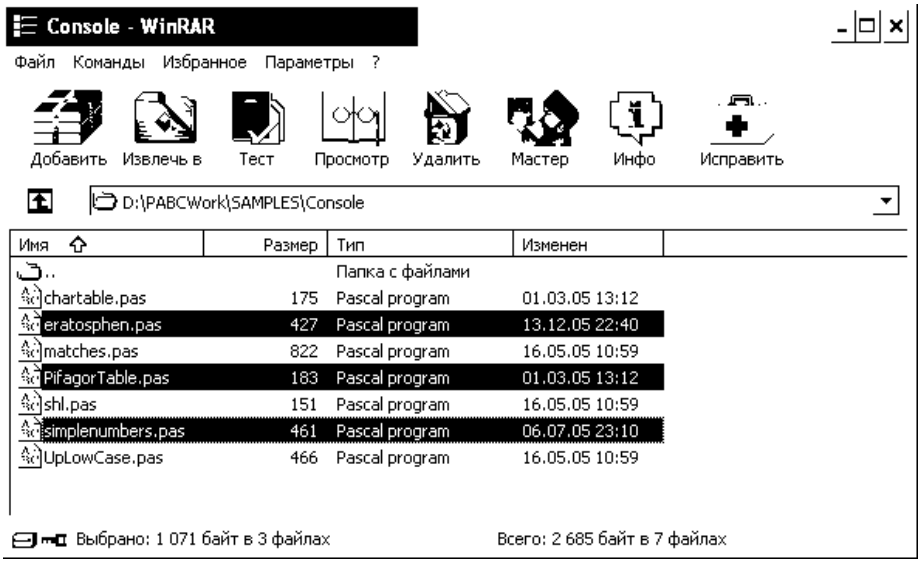
Код и наименование индикатора достижения компетенции	Образовательный результат
ОПК-5.1: Оформляет техническую документацию при выполнении задач профессиональной деятельности согласно стандартам	**Обучающийся умеет:** определять и анализировать угрозы безопасности информации в зависимости от среды эксплуатации продуктов информационных технологий; использовать современные программные средства для защиты информации; принимать адекватные решения при выборе средств защиты информации на основе анализа угроз; разрабатывать и создавать типовые схемы защиты информации на основе современных средств обеспечения информационной безопасности; обоснованно выбирать соответствующие организационные и программно-аппаратные средства для организации систем информационной защиты.

Примеры заданий

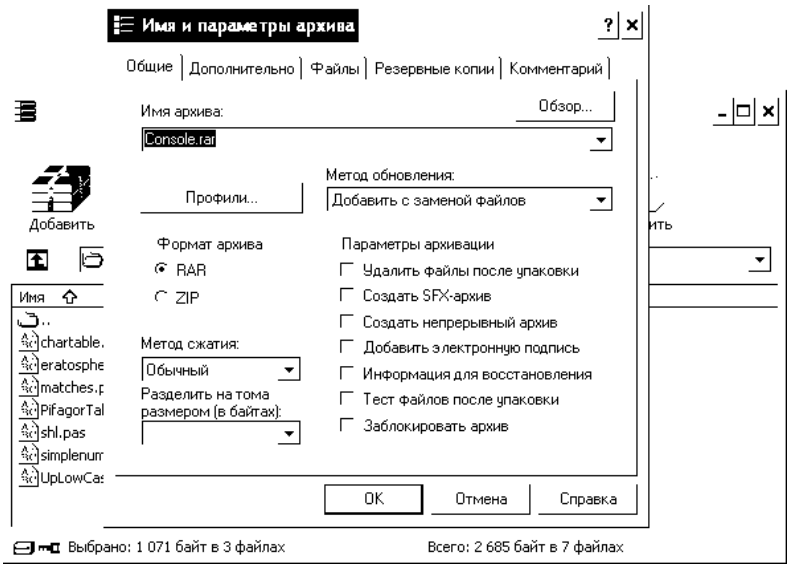
Задание 1

Архивация данных

1. Запустите программу резервного копирования, например, «Архивация данных», WinRar, Хранитель V и т.п.
2. Выберите необходимые документы для резервного копирования.

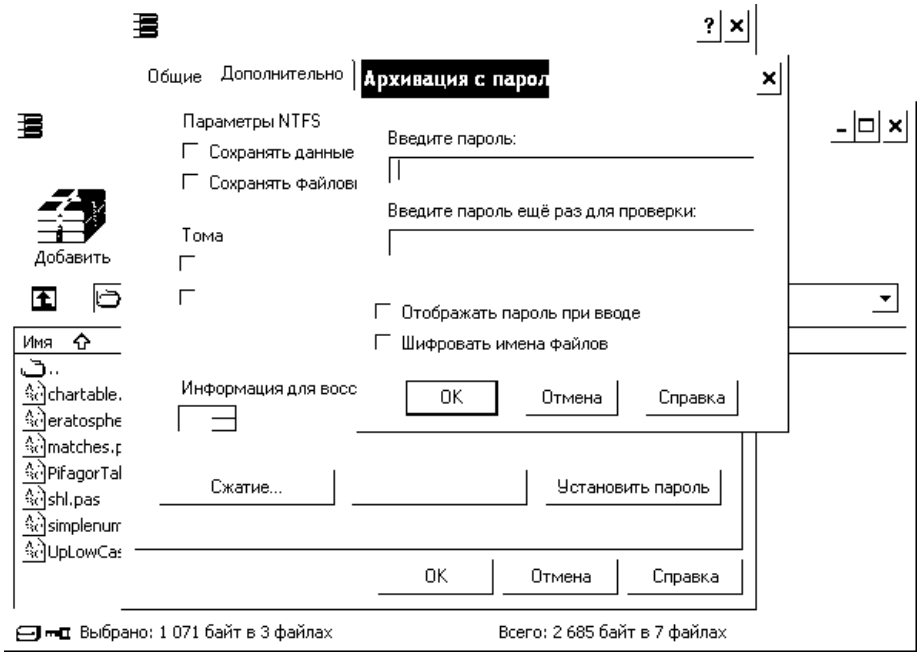


3. Нажмите кнопку «Добавить».
4. На вкладке «Общие» укажите имя архивного файла.



5. Выберите необходимый метод сжатия.

6. На вкладке «Дополнительно» нажмите кнопку «Установить пароль» и в открывшемся окне укажите пароль для выбранных файлов, добавляемых в указанный архив.
7. Ознакомьтесь с остальными параметрами, расположенными на вкладках «Общие», «Дополнительно», «Резервные копии», «Комментарии» окна «Имя и параметры архива» программы WinRar. Задайте необходимые параметры.
8. Нажмите кнопку «OK», после чего в заданный архив будут добавлены выбранные файлы.
9. Убедитесь, что для просмотра содержимого добавленных файлов архива, необходимо ввести пароль.



Задание 2

1. Выполнить настройку программы: выбрать метод шифрования; ввести ключи для всех методов; ввести вероятное слово; осуществить все остальные системные настройки.

Задание 3

2. Для метода замены (одноалфавитного метода): выбрать данный алгоритм в списке доступных методов шифрования;⎪ установить необходимое смещение;⎪ открыть произвольный файл;⎪ просмотреть содержимое исходного файла;⎪ выполнить для этого файла шифрование (при необходимости можно задать⎪ имя зашифрованного файла); просмотреть в редакторе зашифрованный файл;⎪ ввести вероятное слово;⎪ ввести вероятную длину ключа (кроме метода замены);⎪ подобрать ключ;⎪ выполнить расшифрование со всеми найденными ключами;⎪ найти в каком-либо из расшифрованных файлов правильно⎪ расшифрованное ключевое слово;⎪ расшифровать файл исходным ключом;⎪ проверить результат⎪ В отчете для каждого метода шифрования описывается последовательность выполняемых действий, имена всех использованных файлов, указываются исходные и найденные ключи, описывается процесс дешифрования. Преподавателю предоставляется отчет о проделанной работе и все использованные файлы

ОПК-3.3 : Составляет обзоры, аннотации, рефераты, научные доклады, публикации и библиографии по научно-исследовательской работе с учетом требований информационной безопасности	**Обучающийся умеет:** решать сложные поставленные задачи, применяя принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности, подготавливать обзоры, аннотации.

Примеры заданий

Задание 4

Разработать и реализовать на языке php модуль web-сайта, отображающий данные из БД «Список продуктов».

Задание 5

Для заданного преподавателем варианта информационной системы в организации:

- классифицировать ИСПДн по уровням защищённости;
- разработать модель потенциальных угроз;
- используя одну из стандартных методик провести оценку рисков и сформировать на её основе список актуальных угроз;
- разработать одну из политик безопасности для данного объекта;

Оформить отчёт о выполненной работе. Оценка выставляется на основании отчёта. При необходимости преподаватель может назначить дополнительно устную защиту.

ПК-5.1: Оформляет техническую документацию при выполнении задач профессиональной деятельности согласно стандартам	**Обучающийся владеет:** навыками разработки защищенных приложений; навыками создания защищенной среды спомощью аппаратно-программных средств защиты; навыками самостоятельного проектирования систем защиты информации; методами оценки эффективности систем защиты информации в компьютерныхсистемах..

Примеры заданий

Задание 6

- Произвести настройку аудита локальной системы на ПК.
- Просмотреть события, происходящие в Вашей системе.
- Проанализировать текущие параметры Вашей системы.
- Просмотреть состояние сетевых соединений в Вашей системы.

Задание 7

Для одноалфавитного метода с фиксированным смещением определить установленное в программе смещение.

Для этого:

- просмотреть предварительно созданный с помощью редактора свой текстовый файл;
- выполнить для этого файла шифрование;
- просмотреть в редакторе зашифрованный файл;
- просмотреть гистограммы исходного и зашифрованного текстов,
- описать гистограммы (в чем похожи, чем отличаются) и определить, с каким смещением было выполнено шифрование;
- расшифровать зашифрованный текст:

1) с помощью программы, после чего проверить в редакторе правильность расшифрования;
2) вручную с помощью гистограмм; описать и объяснить процесс дешифрования.

Для одноалфавитного метода с задаваемым смещением (шифр Цезаря):

- для своего исходного текста выполнить шифрование с произвольным смещением;
- просмотреть и описать гистограммы исходного и зашифрованного текстов, определить смещение для нескольких символов;
- расшифровать текст с помощью программы;
- имеется зашифрованный шифром Цезаря текст; дешифровать его с помощью программы методом подбора смещения;
- указать, с каким смещением был зашифрован файл.

В отчете для каждого метода шифрования описывается последовательность выполняемых действий, имена всех использованных файлов, описываются полученные гистограммы, указывается найденное смещение, описывается процесс дешифрования. Преподавателю предоставляется отчет о проделанной работе и все использованные и созданные файлы

Задание 8

Подробно опишите реально существующее или вымышленное малое предприятие: сферу деятельности, состав и структуру информационной системы, особенности организации процесса защиты информации, применяемые методы и средства.

С помощью программы MSAT проведите оценку рисков для предприятия.

ПК-3.3 : Составляет обзоры, аннотации, рефераты, научные доклады, публикации и библиографии по научно-исследовательской работе с учетом требований информационной безопасности	**Обучающийся владеет:** навыками составления рефератов, научные докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.

Примеры заданий

Задание 9

Заполнить таблицу «Перечень видов тайн», рассмотрев не менее 30 видов тайн. Дополнить таблицу описанием сфер деятельности, в которых пользователь может столкнуться с тем или другим видом тайны.

Для заданного преподавателем варианта информационной системы в организации:

- классифицировать ИСПДн по уровням защищённости;
- разработать модель потенциальных угроз;
- используя одну из стандартных методик провести оценку рисков и сформировать на её основе список актуальных угроз;
- разработать одну из политик безопасности для данного объекта;

Оформить отчёт о выполненной работе. Оценка выставляется на основании отчёта. При необходимости преподаватель может назначить дополнительно устную защиту.

№	Сведения	Ссылка на НПА		Термин / Комментарии
		Основание	Наказание за разглашение	
1.	Государственная тайна	Конституция РФ ст.29 п.4 ФЗ №5485-1 ст.5 УП №1203 149-ФЗ ст.9 п.3	УК РФ ст.275, 276, 283, 283.1, 284 ТК РФ ст.81 6)в) (разглашение охраняемой законом тайны) ТК РФ ст.243 7) (случаи полной материальной ответственности) КоАП ст.13.12 п.7 (нарушение правил защиты информации)	***«Государственная тайна** - защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности РФ.» - ФЗ №5485-1* Общий перечень сведений представлен в «ФЗ о ГТ», детализированный представлен в перечне, утвержденном Указом Президента РФ
2.	Коммерческая тайна	98-ФЗ ГК РФ IV ст.1465	УК РФ ст.183 УК РФ ст.147	98-ФЗ «… режим КТ в отношении информации, составляющей секрет производства (ноу-хау)»

Задание. 10

1) Разработать презентацию «Цели, задачи, предпосылки и направления организационной и управленческой работы в сфере информационной безопасности».

2) Разработать презентацию «Основные понятия и определения в сфере информационной безопасности».

2.3 Примерный перечень тем курсовых работ

1. Сравнительный анализ инструментальных средства анализа рисков информационной безопасности.
2. Сравнительный анализ методов аутентификации пользователей.
3. Анализ информационной агрессии в социальных сетях.
4. Сравнительный анализ способов информационного воздействия в сети Интернет.
5. Разработка программы шифрования данных методом перестановки.
6. Разработка программы шифрования данных методом гаммирования.
7. Разработка программы шифрования данных методом замены.
8. Разработка программы шифрования данных аналитическим методом.
9. Оценка угроз информационного воздействия с использованием метода анализа иерархий.
10. Использование методики комплексного оценивания для определения уровня информационного воздействия.
11. Разработка программы для скрытия и извлечение информации в графических файлах.
12. Разработка программы для скрытие и извлечение информации в звуковых файлах.
13. Разработка программы для скрытие и извлечение информации в видеофайлах.
14. Разработка программы для скрытие и извлечение информации в текстовых файлах.
15. Использование математических методов для оценки информационных угроз безопасности личности (предприятия).
16. Использование DLP-систем для осуществления контроля каналов коммуникаций предприятия.
17. Обеспечение защиты корпоративных информационных ресурсов от утечек информации при помощи DLP-систем.
18. Управление инцидентами информационной безопасности с использованием возможностей DLP-систем.
19. Практические аспекты использования инструментов аналитики в DLP-системах.

20. Анализ схем мошенничества в сети Интернет
21. Анализ схем мошенничества с банковскими картами.
22. Защита пользовательских данных на портативных устройствах
23. Использование метода анализа иерархий для оценки безопасности социальных сетей
24. Разработка политики резервного копирования для предприятия
25. Сравнительный анализ систем резервного копирования
26. Информационная безопасность, как элемент конкурентоспособности организации
27. Обоснование выбора информационной системы для внедрения на предприятии с учетом информационной безопасности.
28. Разработка корпоративной методики анализа рисков
29. Цифровые следы при работе с электронными устройствами.

2.4. Перечень вопросов для подготовки обучающихся к промежуточной аттестации (экзамен)

1. Компьютерная информация: определение, основные категории с точки зрения безопасности
2. Основные категории безопасности информационных систем. Регламентирующие документы и стандарты в области компьютерной безопасности. Критерии надежности систем, классы безопасности.
3. Правовые основы защиты информации в РФ, Обзор законов РФ в области информационной безопасности.
4. Дискреционная и мандатная модель доступа к объектам информационных систем.
5. Классификация угроз информационным системам. Фундаментальные, базовые и первичные угрозы
6. Механизмы реализации услуг безопасности в информационных системах
7. Классификация криптографических алгоритмов
8. Структурная схема симметричной криптосистемы
9. Структурная схема асимметричной криптосистемы
10. Математические определения шифра, процедур шифрования и дешифрации
11. История развития криптоалгоритмов: шифр Цезаря, афинная криптосистема, шифры Виженера и Вернома
12. Частотный криптоанализ одно- и многопоточных шифров
13. Понятие секретности криптоалгоритма. Разновидности атак на криптоалгоритмы
14. Блочное симметричное шифрование, обратимые и необратимые, линейные и нелинейные преобразования
15. Принцип итерирования как основной принцип построения современных блочных шифров. SP-сеть, сеть Фейштеля
16. Алгоритм шифрования TEA: структура, достоинства и недостатки
17. Режимы шифрования блочных шифров ECB, CBC, CFB, OFB
18. Методы криптоанализа блочных шифров
19. Поточные шифры: принципы функционирования, структура
20. Методы построения нелинейных поточных шифров
21. Асимметричные криптосистемы: принципы функционирования, трудно вычислимые математические задачи, определяющие криптостойкость асимметричных криптоалгоритмов
22. RSA: структура криптоалгоритма
23. Метод ключевого обмена Диффи-Хелмана
24. Хэш-функции: назначение и основные свойства
25. Итеративно-последовательная схема построения хэш-функций. Хэш-функции на основе блочных шифров
26. Электронная цифровая подпись: назначение, структура системы ЭЦП на основе алгоритма RSA
27. Инфораструктура PKI.Сертификация ключей асимметричных систем шифрования. Структура сертификата.
28. Иерархическая и сетевая модель сертификации ключей асимметричных систем шифрования.
29. Обзор современных защищенных сетевых протоколов.
30. Угрозы безопасности в глобальных сетях

31. Межсетевые экраны: назначение, основные функции, состав
32. Пакетные фильтры: назначение, основные принципы формирования правил фильтрации, достоинства и недостаткиProxy-сервера : назначение, основные функции, достоинства и недостатки
33. Архитектура современных межсетевых экранов: двухканальный компьютер, экранированный узел, демилитаризованная зона
34. Определение вредоносной программы. Классификация вредоносных программ.
35. Компьютерные вирусы: разновидности, используемые методы заражения.
36. Сетевые черви: определение, способы распространения.
37. Троянская программа: назначение, классификация, руткиты как средство маскировки.
38. Методики защиты от вредоносных программ.
39. Модель безопасности ОС Windows. . Реализация дискреционной модели защиты доступа к ресурсам системы.
40. Аудит событий безопасности современных операционных систем.
41. Модель безопасности ОС Windows. Идентификация пользователей: идентификатор безопасности и маркер доступа субъекта, привилегии.
42. Шифрующая файловая система (EFS): принцип работы, структура зашифрованного файла, роль агентов восстановления.

3. Методические материалы, определяющие процедуру и критерии оценивания сформированности компетенций при проведении промежуточной аттестации

Критерии формирования оценок по ответам на вопросы, выполнению тестовых заданий

- оценка **«отлично»** выставляется обучающемуся, если количество правильных ответов на вопросы составляет 100 – 90 % от общего объёма заданных вопросов;

- оценка **«хорошо»** выставляется обучающемуся, если количество правильных ответов на вопросы – 89 – 76 % от общего объёма заданных вопросов;

- оценка **«удовлетворительно»** выставляется обучающемуся, если количество правильных ответов на тестовые вопросы –75–60 % от общего объёма заданных вопросов;

- оценка **«неудовлетворительно»** выставляется обучающемуся, если количество правильных ответов – менее 60 % от общего объёма заданных вопросов.

Критерии формирования оценок по результатам выполнения заданий

«Зачтено» – ставится за работу, выполненную полностью без ошибок и недочетов в соответствии с заданием. Обучающийся полностью владеет информацией по теме работы, решил все поставленные в задании задачи**.**

«Не зачтено» - ставится за работу, если обучающийся правильно выполнил менее 2/3 всего задания, использовал при выполнении неправильные алгоритмы, допустил грубые ошибки при программировании, сформулировал неверные выводы по результатам работы.

Виды ошибок:

- грубые ошибки: незнание основных понятий, правил, норм; незнание приемов решения задач; ошибки, показывающие неправильное понимание условия предложенного задания.

- негрубые ошибки: неточности формулировок, определений; нерациональный выбор хода решения.

- недочеты: нерациональные приемы выполнения задания; отдельные погрешности в формулировке выводов; небрежное выполнение задания.

Критерии формирования оценок по написанию и защите курсовой работы

«Отлично» *(5 баллов)* – получают обучающиеся, оформившие курсовую работу в соответствии с предъявляемыми требованиями, в которой отражены все необходимые результаты проведенного анализа, сделаны обобщающие выводы и предложены рекомендации в соответствии с тематикой курсовой работы, а также грамотно и исчерпывающе ответившие на все встречные вопросы преподавателя.

«Хорошо» *(4 балла)* – получают обучающиеся, оформившие курсовую работу в соответствии с предъявляемыми требованиями, в которой отражены все необходимые результаты проведенного анализа, сделаны обобщающие выводы и предложены рекомендации в соответствии с тематикой курсовой работы. При этом при ответах на вопросы преподавателя обучающийся допустил не более двух ошибок.

«Удовлетворительно» *(3 балла)* – получают обучающиеся, оформившие курсовую работу в соответствии с предъявляемыми требованиями. При этом при ответах на вопросы преподавателя обучающийся допустил более трёх ошибок.

«Неудовлетворительно» *(0 баллов)* – ставится за курсовую работу, если число ошибок и недочетов превысило удовлетворительный уровень компетенции.

Критерии формирования оценок по экзамену

«Отлично» (5 баллов) – обучающийся демонстрирует знание всех разделов изучаемой дисциплины: содержание базовых понятий и фундаментальных проблем; умение излагать программный материал с демонстрацией конкретных примеров. Свободное владение материалом должно характеризоваться логической ясностью и четким видением путей применения полученных знаний в практической деятельности, умением связать материал с другими отраслями знания.

«Хорошо» (4 балла) – обучающийся демонстрирует знания всех разделов изучаемой дисциплины: содержание базовых понятий и фундаментальных проблем; приобрел необходимые умения и навыки, освоил вопросы практического применения полученных знаний, не допустилфактических ошибок при ответе, достаточно последовательно и логично излагает теоретический материал, допуская лишь незначительные нарушения последовательности

изложения и некоторые неточности. Таким образом данная оценка выставляется за правильный, но недостаточно полный ответ.

«Удовлетворительно» (3 балла) – обучающийся демонстрирует знание основных разделов программы изучаемого курса: его базовых понятий и фундаментальных проблем. Однако знание основных проблем курса не подкрепляются конкретными практическими примерами, не полностью раскрыта сущность вопросов, ответ недостаточно логичен и не всегда последователен, допущены ошибки и неточности.

«Неудовлетворительно» (0 баллов) – выставляется в том случае, когда обучающийся демонстрирует фрагментарные знания основных разделов программы изучаемого курса: его базовых понятий и фундаментальных проблем. У экзаменуемого слабо выражена способность к самостоятельному аналитическому мышлению, имеются затруднения в изложении материала, отсутствуют необходимые умения и навыки, допущены грубые ошибки и незнание терминологии, отказ отвечать на дополнительные вопросы, знание которых необходимо для получения положительной оценки.