ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ

Технические способы и методы защиты информации

Код модуля
1158315(1)

Модуль
Экономическая безопасность

Екатеринбург

Оценочные материалы составлены автором(ами):

№ п/п	Фамилия, имя, отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Леонтьева Юлия Владимировна	кандидат экономических наук, доцент	Доцент	финансового и налогового менеджмента
2	Шилков Владимир Ильич	кандидат экономических наук, доцент	Доцент	экономической безопасности производственных комплексов

Согласовано:

Управление образовательных программ Русакова И.Ю.

Авторы:

1. СТРУКТУРА И ОБЪЕМ ДИСЦИПЛИНЫ Технические способы и методы защиты информации

1.	**Объем дисциплины в зачетных единицах**	3	
2.	**Виды аудиторных занятий**	Лекции Практические/семинарские занятия	
3.	**Промежуточная аттестация**	Экзамен	
4.	**Текущая аттестация**	Контрольная работа	1
		Домашняя работа	1

2. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ (ИНДИКАТОРЫ) ПО ДИСЦИПЛИНЕ МОДУЛЯ Технические способы и методы защиты информации

Индикатор – это признак / сигнал/ маркер, который показывает, на каком уровне обучающийся должен освоить результаты обучения и их предъявление должно подтвердить факт освоения предметного содержания данной дисциплины, указанного в табл. 1.3 РПМ-РПД.

Таблица 1

Код и наименование компетенции	**Планируемые результаты обучения (индикаторы)**	**Контрольно-оценочные средства для оценивания достижения результата обучения по дисциплине**
1	**2**	**3**
ПК-5 -Способность применять методы осуществления контроля финансово-хозяйственной деятельности хозяйствующих субъектов	З-1 - Объяснять понятие сущность и задачи основных форм и методов проведения финансового, налогового, валютного, таможенного и других видов контроля П-2 - Организовать и осуществлять мониторинг деятельности организаций, отдельных сегментов рынка и экономики в целом с целью выявления объектов повышенного риска У-2 - Применять прогрессивные методы и инструменты контроля к конкретным объектам проверки, в том числе методы внутреннего финансового контроля	Домашняя работа Контрольная работа Лекции Практические/семинарские занятия Экзамен

3. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ МОДУЛЯ В БАЛЬНО-РЕЙТИНГОВОЙ СИСТЕМЕ (ТЕХНОЛОГИЧЕСКАЯ КАРТА БРС)

3.1. Процедуры текущей и промежуточной аттестации по дисциплине

1. Лекции: коэффициент значимости совокупных результатов лекционных занятий – 0.5		
Текущая аттестация на лекциях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
домашняя работа	9,18	*50*
контрольная работа	9,9	*50*
Весовой коэффициент значимости результатов текущей аттестации по лекциям – 0.5		
Промежуточная аттестация по лекциям – экзамен **Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – 0.5**		
2. Практические/семинарские занятия: коэффициент значимости совокупных результатов практических/семинарских занятий – 0.4		
Текущая аттестация на практических/семинарских занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
активность на занятиях	9,18	100
Весовой коэффициент значимости результатов текущей аттестации по практическим/семинарским занятиям– 1		
Промежуточная аттестация по практическим/семинарским занятиям–нет **Весовой коэффициент значимости результатов промежуточной аттестации по практическим/семинарским занятиям– не предусмотрено**		
3. Лабораторные занятия: коэффициент значимости совокупных результатов лабораторных занятий –не предусмотрено		
Текущая аттестация на лабораторных занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Весовой коэффициент значимости результатов текущей аттестации по лабораторным занятиям -не предусмотрено		
Промежуточная аттестация по лабораторным занятиям –нет **Весовой коэффициент значимости результатов промежуточной аттестации по лабораторным занятиям – не предусмотрено**		
4. Онлайн-занятия: коэффициент значимости совокупных результатов онлайн-занятий –не предусмотрено		
Текущая аттестация на онлайн-занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**

Весовой коэффициент значимости результатов текущей аттестации по онлайн-занятиям -не предусмотрено
Промежуточная аттестация по онлайн-занятиям –нет **Весовой коэффициент значимости результатов промежуточной аттестации по онлайн-занятиям – не предусмотрено**

3.2. Процедуры текущей и промежуточной аттестации курсовой работы/проекта

Текущая аттестация выполнения курсовой работы/проекта	**Сроки − семестр, учебная неделя**	**Максимальная оценка в баллах**
Весовой коэффициент текущей аттестации выполнения курсовой работы/проекта– не предусмотрено		
Весовой коэффициент промежуточной аттестации выполнения курсовой работы/проекта– защиты – не предусмотрено		

4. КРИТЕРИИ И УРОВНИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ МОДУЛЯ

4.1. В рамках БРС применяются утвержденные на кафедре/институте критерии (признаки) оценивания достижений студентов по дисциплине модуля (табл. 4) в рамках контрольно-оценочных мероприятий на соответствие указанным в табл.1 результатам обучения (индикаторам).

Таблица 4

Критерии оценивания учебных достижений обучающихся

Результаты обучения	**Критерии оценивания учебных достижений, обучающихся на соответствие результатам обучения/индикаторам**
Знания	Студент демонстрирует знания и понимание в области изучения на уровне указанных индикаторов и необходимые для продолжения обучения и/или выполнения трудовых функций и действий, связанных с профессиональной деятельностью.
Умения	Студент может применять свои знания и понимание в контекстах, представленных в оценочных заданиях, демонстрирует освоение умений на уровне указанных индикаторов и необходимых для продолжения обучения и/или выполнения трудовых функций и действий, связанных с профессиональной деятельностью.
Опыт /владение	Студент демонстрирует опыт в области изучения на уровне указанных индикаторов.
Другие результаты	Студент демонстрирует ответственность в освоении результатов обучения на уровне запланированных индикаторов. Студент способен выносить суждения, делать оценки и формулировать выводы в области изучения. Студент может сообщать преподавателю и коллегам своего уровня собственное понимание и умения в области изучения.

4.2 Для оценивания уровня выполнения критериев (уровня достижений обучающихся при проведении контрольно-оценочных мероприятий по дисциплине модуля) используется универсальная шкала (табл. 5).

Таблица 5

Шкала оценивания достижения результатов обучения (индикаторов) по уровням

Характеристика уровней достижения результатов обучения (индикаторов)				
№ п/п	**Содержание уровня выполнения критерия оценивания результатов обучения (выполненное оценочное задание)**	**Шкала оценивания**		
		Традиционная характеристика уровня		**Качественная характеристика уровня**
1.	Результаты обучения (индикаторы) достигнуты в полном объеме, замечаний нет	Отлично (80-100 баллов)	Зачтено	Высокий (В)
2.	Результаты обучения (индикаторы) в целом достигнуты, имеются замечания, которые не требуют обязательного устранения	Хорошо (60-79 баллов)		Средний (С)
3.	Результаты обучения (индикаторы) достигнуты не в полной мере, есть замечания	Удовлетворительно (40-59 баллов)		Пороговый (П)
4.	Освоение результатов обучения не соответствует индикаторам, имеются существенные ошибки и замечания, требуется доработка	Неудовлетворительно (менее 40 баллов)	Не зачтено	Недостаточный (Н)
5.	Результат обучения не достигнут, задание не выполнено	Недостаточно свидетельств для оценивания		Нет результата

5. СОДЕРЖАНИЕ КОНТРОЛЬНО-ОЦЕНОЧНЫХ МЕРОПРИЯТИЙ ПО ДИСЦИПЛИНЕ МОДУЛЯ

5.1. Описание аудиторных контрольно-оценочных мероприятий по дисциплине модуля

5.1.1. Лекции

Самостоятельное изучение теоретического материала по темам/разделам лекций в соответствии с содержанием дисциплины (п. 1.2. РПД)

5.1.2. Практические/семинарские занятия

Примерный перечень тем

1. Угрозы в информационных сетях
2. Безопасность операционных систем
3. Безопасность программного обеспечения
4. Способы и средства защиты информации
5. Основы кодирования информации
6. Математические основы криптографии
7. Криптографические методы защиты информации
8. Сетевые средства защиты информации

9. Управление рисками информационной безопасности

LMS-платформа − не предусмотрена

5.2. Описание внеаудиторных контрольно-оценочных мероприятий и средств текущего контроля по дисциплине модуля

Разноуровневое (дифференцированное) обучение.

Базовый

5.2.1. Контрольная работа

Примерный перечень тем

1. Разработать мероприятия по эффективному использованию технических средств регламентации и управления доступом к защищаемой информации

2. Разработать систему контроля инженерно-технической защиты режимного предприятия

3. Разработать модель способов физического проникновения злоумышленника к источникам информации

4. Разработать функциональную и информационные модели для описания динамики канала утечки информации

5. Разработать структурную и пространственные модели для описания статики канала утечки информации

6. Разработать мероприятия по информационному и энергетическому скрытию информации на режимном предприятии

7. Разработать систему информационно-технических мероприятий по повышению эффективности систем защиты в компьютерных сетях

8. Разработать систему информационно-технических мероприятий по снижению рисков утечки информации по аудио каналам

9. Разработать систему информационно-технических мероприятий по снижению рисков утечки информации по оптическим каналам

10. Разработать систему информационно-технических мероприятий по снижению рисков утечки информации по электро-магнитным каналам

Примерные задания

Министерство высшего образования и науки Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования «Уральский федеральный университет имени первого
Президента России Б.Н. Ельцина» (УрФУ)
Школа экономики и управления
Кафедра экономической безопасности производственных комплексов

Технические способы и методы защиты информации

Контрольная работа

Методы обеспечения информационно-экономической безопасности

элементов критической инфраструктуры умного города (“Smart City”)

Выполнил студент 5 курса:

Иванов А.А.

Группа ЭУ-583583

Преподаватель:

Петров В.В.

Екатеринбург 2022

ЗАДАНИЕ
к контрольной работе:
Методы обеспечения информационно-экономической безопасности
элементов критической инфраструктуры умного города (“Smart City”)

1) Назвать перспективные направления внедрения информационных систем и технологий для управления умными городами;
2) Сформулировать основные цели и задачи элементов критической информационной структуры умного города;
3) Определить основные информационные, экономические и организационно-технические риски умных городов;
4) Назвать нуждающиеся в защите наиболее уязвимые компоненты информационной структуры умных городов;
5) Назвать основные направления повышения уровня информационно-экономической безопасности компонентов информационной структуры умного города.

Фрагмент ответа на вопрос 3:

Внедрение информационно-коммуникационных технологий в критические инфраструктуры управления городским хозяйством, наряду с достижением положительных социально-экономических эффектов, в ряде случаев, может приводить к возникновению дополнительных рисков и угроз, в том числе и для информационно-экономической безопасности умного города.

К рискам умного города отнесены риски: «катастрофических инцидентов», «снижения культурного развития», «утечки данных», «технической неисправности», «электронного неравенства», «полной зависимости от техники», «снижения уровня образования».

Так, например, к группе *технологических рисков* можно отнести несколько рисков, в том числе:

- неконтролируемое развитие искусственного интеллекта;
- угрозы кибербезопасности и уязвимость информационных систем;
- угрозу потери данных, устаревшую архитектуру для новых технологий.

К группе социальных рисков можно отнести в том числе:

- усиление цифрового разрыва между «умными» и остальными городами.
- развитие кибертерроризма и хакерства;
- сохранение предпочтений к использованию неэлектронных технологий;

Сбои и отказы в работе систем управления умным городом следует связывать, с рисками снижения информационно-экономической безопасности.

Фрагмент ответа на вопрос 5:

Для повышения уровня информационной безопасности *умного города* могут быть рекомендованы *тестирование и оценка* опасности возникновения специфических угроз со стороны новых:

- информационных технологий (программно-технологические компоненты);
- организационно-управленческих мероприятий (организационные процедуры и процессы преобразования информации);
- источников информации (возможной недостоверности и ненадежности данных);
- целей использования информации (альтернативного использования данных);
- пользователей и обслуживающего персонала.

Для снижения уровня рисков для информационной безопасности *умного города* со стороны *человеческого фактора*, целесообразно:

- организовать обучение персонала и пользователей;
- обеспечить проведение мероприятий по усилению контроля над действиями пользователей и персонала.

В числе комплекса различных мероприятий, предотвратить несанкционированный доступ к базам данных, оборудованию и каналам связи *может* внедрение криптографических методов защиты.

LMS-платформа − не предусмотрена

5.2.2. Домашняя работа

Примерный перечень тем

1. Криптографические средства защиты информации в стандарте GSM и их стойкость
2. Исследование алгоритма поточного шифрования RC4
3. Особенности применения цифровой подписи вслепую в протоколах электронного тайного голосования
4. Новые американские стандарты режимов шифрования с аутентификацией
5. Схемы криптосистем на основе парных отображений
6. Методы эффективной реализации схем электронной цифровой подписи на основе группы точек эллиптических кривых
7. Возможности преобразования отечественного стандарта цифровой подписи в схему цифровой подписи вслепую
8. Сравнение криптографических средств различных протоколов мобильных платежей

9. Исследование свойств подстановок на двоичных векторах при малых размерностях и их применение при построении узлов алгоритмов шифрования

10. Решение проблемы повторной траты (https://ru.wikipedia.org/wiki/Двойное_расходование) криптографическими методами в схемах электронных платежей.

11. Анализ подходов к ролевому управлению доступом

12. Аудит безопасности информационной системы с использованием теста на проникновение

13. Аудит информационной безопасности

14. Выявление нарушений законодательства в сети Интернет

15. Выявление признаков, определяющих группы по интересам

16. Шифрование информации. Цель, место, применение

17. Защита информации предприятия от утечки по техническим каналам

18. Защита конфиденциальной информации на предприятиях по формам собственности

19. Защита персональных данных на предприятиях

20. Криптографические методы защиты информации

21. Криптоанализ алгоритмов: Hughes XPD/KPD, Nanoteq

22. Криптоанализ генераторов: «стоп-пошёл» Both-Piper, DNRSG, Геффа, Джен-нингса, каскад Голлманна

23. Криптоанализ потоковых шифров: Gifford, A5, LFSR

24. Защита информационной и интеллектуальной собственности

25. Информационные угрозы предпринимательству

26. Исследование проблем информационной безопасности и защита информации террито-риально разнесенных центров обработки данных

27. Исследование проблем информационной безопасности мобильного доступа

28. Исследование тенденций развития межсетевых экранов прикладного уровня

29. Линейная сложность генераторов на базе LFSR

30. Место DLP-систем (предотвращение утечек, Data Leak Prevention) в современной структуре обеспечения информационной безопасности автоматизированной информационной системы

Примерные задания

Министерство высшего образования и науки Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования «Уральский федеральный университет имени первого Президента России Б.Н. Ельцина» (УрФУ)
Школа экономики и управления
Кафедра экономической безопасности производственных комплексов

Домашнее задание по дисциплине:

Технические способы и методы защиты информации

На тему:

Место DLP-систем (предотвращение утечек, Data LeakPrevention) в современной структуре обеспечения информационной безопасности автоматизированной информационной системы.

Выполнил студент 5 курса:

Иванов А.А.

Группа ЭУ-583583

Преподаватель:

Петров В.В.

Екатеринбург 2022

Содержание

Хостовая DLP система (рисунок 2) основана на использовании специализированных программ (агентов), которые устанавливаются на конечных узлах сети – рабочих станциях, серверах приложений и т.д. Агенты играют сразу две роли. С одной стороны, они производят контроль деятельности пользователей компьютеров, не позволяя им нарушить политику безопасности (например, запрещая копировать любые файлы на внешний носитель).

Рисунок 2 – Хостовая DLP система.

С другой - регистрируют все действия операторов и передают их в централизованное хранилище, позволяя службе безопасности получать полную картину происходящего. Использование агентов ограничивает сферу применения хостовых DLP-систем: они способны видеть лишь локальные или сетевые устройства, подключенные непосредственно к тем компьютерам, на которых они работают.

Глава 3. Функционирование и модель DLP систем

3.1 Принципы функционирования

В последнее время упоминания об утечках информации из самых разных–коммерческих, некоммерческих, государственных и пр. организаций ~~вновостных лентахинформационных агенств~~ и Интернет

15

LMS-платформа − не предусмотрена

5.3. Описание контрольно-оценочных мероприятий промежуточного контроля по дисциплине модуля

5.3.1. Экзамен

Список примерных вопросов

1. Концепция информационной безопасности
2. Виды угроз. Внутренние и внешние источники угроз
3. Организационно-правовое обеспечение информационной безопасности
4. Угрозы в информационных системах
5. Способы защиты информации
6. Средства защиты информации
7. Компьютерные вирусы и антивирусные программы
8. Государственные стандарты по информационной безопасности
9. Понятие информационной безопасности. Угрозы. Механизмы анализа угроз. Инструментарий построения рубежей
10. Основы криптографии. Шифрование и кодирование. Общие принципы и модели

11. Защита от несанкционированного доступа

12. Простые шифры. Шифр простой замены. Шифр Цезаря (шифр сдвига, код Цезаря, сдвиг Цезаря)

13. Шифр вертикальной перестановки (перестановочный шифр, шифрограмма по вертикалям)

14. Гаммирование (метод симметричного шифрования)

15. Методы расшифровки зашифрованной информации. Основные способы криптоанализа простых шифров

16. Основные методы криптоанализа. Атака на основе шифротекста, открытых текстов и соответствующих шифротекстов, подобранного открытого текста, адаптивно подо-бранного открытого текста

17. Дополнительные методы криптоанализа. Атака на основе подобранного шифротекста, подобранного ключа. Бандитский криптоанализ

18. Симметричные криптосистемы. Схема, сеть Фейстеля (Horst Feistel, Feistel network, Feistel cipher). Стандарты блочного шифрования. Федеральный стандарт DES

19. Симметричные криптосистемы. Алгоритм шифрования ГОСТ 28147-89 (Магма), ГОСТ Р 34.12-2015 (Кузнечик). режимы шифрования и гаммирования

20. Симметричные криптосистемы. Алгоритм блочного шифрования Rijndael - Advanced Encryption Standard (AES)

21. Атаки на блочные шифры. Дифференциальный криптоанализ. Дифференциальный криптоанализ на основе отказов устройства

22. Атаки на блочные шифры. Линейный криптоанализ. Силовая атака на основе распре-деленных вычислений

23. Поточные шифры. Регистры сдвига с обратной связью. Алгоритм поточного шифрования RC4 (Rivest cipher 4, Ron’s code; ARC4, ARCFOUR)

24. Основные теоремы теории чисел. Проверка числа на простоту. Эффективные алгоритмы возведения в степень

25. Криптосистема RSA (Rivest-Shamir-Adleman — криптографический алгоритм с откры-тым ключом). Устройство RSA. Эффективность реализации. Криптостойкость RSA

26. Атаки на криптосистему RSA. Атака на основе выбранного шифр текста. Атака на основе общего RSA модуля. Раскрытие малого показателя шифрования

LMS-платформа − не предусмотрена

5.4 Содержание контрольно-оценочных мероприятий по направлениям воспитательной деятельности

Направление воспитательной деятельности	Вид воспитательной деятельности	Технология воспитательной деятельности	Компетенция	Результаты обучения	**Контрольно-оценочные мероприятия**
Профессиональное воспитание	учебно-исследовательская, научно-исследовательская	Технология самостоятельной работы	ПК-5	П-2	Лекции Практические/семинарские занятия