

**ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
ПО ДИСЦИПЛИНЕ**
Информационная безопасность

Код модуля
1144713

Модуль
Информационное обеспечение профессиональной
деятельности

Екатеринбург

Оценочные материалы составлены автором(ами):

№ п/п	Фамилия, имя, отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Крылов Виктор Гаврилович	без ученой степени, без ученого звания	Старший преподаватель	региональной экономики, инновационного предпринимательства и безопасности
2	Шкурко Валентина Евгеньевна		старший преподаватель	региональной экономики, инновационного предпринимательства и безопасности

Согласовано:

Управление образовательных программ

И.Ю. Русакова

Авторы:

- Шкурко Валентина Евгеньевна, старший преподаватель, региональной экономики, инновационного предпринимательства и безопасности

1. СТРУКТУРА И ОБЪЕМ ДИСЦИПЛИНЫ Информационная безопасность

1.	Объем дисциплины в зачетных единицах	4	
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 Информационная безопасность

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-4 -Способен обеспечивать условия защиты ресурсов организации от внешних и внутренних угроз экономической безопасности	З-1 - Знать понятия внешних и внутренних угроз экономической безопасности З-2 - Знать методики защиты ресурсов организации от внешних и внутренних угроз экономической безопасности П-1 - Владеть методиками защиты ресурсов организации от внешних и внутренних угроз экономической безопасности У-1 - Уметь применять методики защиты ресурсов организации от внешних и внутренних угроз экономической безопасности	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
<i>контрольная работа</i>	6,16	100
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 – 0.5		
Текущая аттестация на практических/семинарских занятиях	Сроки – семестр, учебная неделя	Максимальная оценка в баллах
<i>домашняя работа</i>	6,16	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. Анализ нормативных документов и стандартов информационной безопасности
 2. Классификация угроз информации и информационным технологиям. Этичный хакинг.
 3. Установка и управление антивирусным программным обеспечением
 4. Установки локальной политики безопасности
 5. Шифрование локальных документов
 6. Настройка персонального межсетевого экран (брандмауэр, файрвол – Brandmauer, Firewall)
 7. Анализ рисков по данным лог-файлов событий
- 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. Анализ нормативных документов и стандартов информационной безопасности
2. Классификация угроз информации и информационным технологиям. Этический хакинг.
3. Установка и управление антивирусным программным обеспечением
4. Установки локальной политики безопасности
5. Шифрование локальных документов
6. Настройка персонального межсетевого экран (брандмауэр, файрвол – Brandmauer, Firewall)
7. Анализ рисков по данным лог-файлов событий

Примерные задания

Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?

- А. Сотрудники;
- Б. Хакеры;
- В. Атакующие;
- Г. Контрагенты (лица, работающие по договору).

Информация это -

- А. сведения, поступающие от СМИ;
- Б. только документированные сведения о лицах, предметах, фактах, событиях;
- В. сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;
- Г. только сведения, содержащиеся в электронных базах данных.

Запрещено относить к информации ограниченного доступа:

- А. информацию о чрезвычайных ситуациях;
- Б. информацию о деятельности органов государственной власти;
- В. документы открытых архивов и библиотек;
- Г. все, перечисленное в остальных пунктах.

Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании?

- А. чтобы убедиться, что проводится справедливая оценка;
- Б. это не требуется. Для анализа рисков следует привлекать небольшую группу специалистов, не являющихся сотрудниками компании, что позволит обеспечить беспристрастный и качественный анализ;

В. поскольку люди в различных подразделениях лучше понимают риски в своих подразделениях и смогут предоставить максимально полную и достоверную информацию для анализа;

Г. Поскольку люди в различных подразделениях сами являются одной из причин рисков, они должны быть ответственны за их оценку.

Защита информации это:

А. процесс сбора, накопления, обработки, хранения, распределения и поиска информации;

Б. преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;

В. получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;

Г. деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё.

Естественные угрозы безопасности информации вызваны:

А. деятельностью человека;

Б. воздействиями объективных физических процессов или стихийных природных явлений, независимых от человека;

В. корыстными устремлениями злоумышленников;

Г. ошибками при действиях персонала.

К посторонним лицам нарушителям информационной безопасности относится:

А. персонал;

Б. пользователи;

В. сотрудники службы безопасности;

Г. представители конкурирующих организаций.

Перехват, который заключается в установке подслушивающего устройства в аппаратуру средств обработки информации называется:

А. активный перехват;

Б. пассивный перехват;

В. аудиоперехват;

Г. видеоперехват.

Компьютерным вирусом называется:

А. программа, способная внедряться в другие программы, с возможностью самовоспроизводства.

Б. вид бактерий, разрушающий микросхемы.

В. процесс разрушения информации на неисправном жёстком диске.

Г. мельчайший микроорганизм, возбудитель заразной болезни.

Преднамеренная угроза информационной безопасности:

А. кража;

Б. ошибка разработчика;

- В. повреждение кабеля, по которому идет передача, в связи с погодными условиями;
- Г. наводнение.

Утечка информации – это...

- А. процесс уничтожения информации;
- Б. несанкционированный процесс переноса информации от источника к злоумышленнику;
- В. процесс добровольного раскрытия информации;
- Г. непреднамеренная утрата носителя информации.

К основным составляющим информационной безопасности относят:

- А. доступность, целостность;
- Б. целостность, защищенность, конфиденциальность;
- В. доступность, целостность, конфиденциальность;
- Г. целостность, защищенность.

Окно опасности – это...

- А. промежуток времени от момента, когда появится возможность слабого места и до момента, когда пробел ликвидируется;
- Б. комплекс взаимосвязанных программ для решения задач определенного класса конкретной предметной области;
- В. формализованный язык для описания задач алгоритма решения задачи пользователя на компьютере;
- Г. данного термина не существует.

LMS-платформа – не предусмотрена

5.2.2. Домашняя работа

Примерный перечень тем

1. Анализ нормативных документов и стандартов информационной безопасности
2. Классификация угроз информации и информационным технологиям. Этический хакинг.
3. Установка и управление антивирусным программным обеспечением
4. Установки локальной политики безопасности
5. Шифрование локальных документов
6. Настройка персонального межсетевого экран (брандмауэр, файрвол – Brandmauer, Firewall)
7. Анализ рисков по данным лог-файлов событий

Примерные задания

Студентам предлагается подготовить и сделать доклад (в виде презентации) по выбранной теме.

Объем работы задается временем, отводимым на презентацию – до 10 минут.

Темы:

- 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, Дженнингса, каскад Голлманна
23. Криптоанализ потоковых шифров: Gifford, A5, LFSR

LMS-платформа – не предусмотрена

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

5.3.1. Экзамен

Список примерных вопросов

1. 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 подобранного 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 (Мagma), ГОСТ Р 34.12-2015 (Кузнечик). режимы шифрования и гаммирования. 23 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 распределенных 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 открытым 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. 27. Криптосистема Эль-Гамала (Elgamal). Вычисление и проверка подписи. Шифрование и дешифрование. Эффективность реализации. 28. Метод экспоненциального ключевого обмена Диффи-Хелмана. Протокол ключевого обмена для нескольких участников. 29. Хеш-функции. Понятие хеш-функции. Основные свойства односторонних функций. MD4 (Message Digest 4), RFC 1186 (The MD4 Message Digest Algorithm). 30. Цифровая подпись. Понятие цифровой подписи. Основные принципы и отличия от реальной подписи. Алгоритмы цифровой подписи - ГОСТ Р 34.10-2012. DSS (Digital Signature Standard). 31. Закон об электронной цифровой подписи в России. Удостоверяющие центры. 32. Протоколы генерации ключей. Случайные ключи. Протоколы распределения ключей. 33. Разделение секрета. Схема разделения секрета Шамира. 34. Применение помехоустойчивых кодов в криптографии. Недвоичные циклические коды Рида-Соломона (Reed-Solomon codes). 35. Верифицируемое разделение секрета. 36. «Шарады» с временным замком (Time-lock puzzles and timed-release Crypto). Построение «шарад» с временным замком. Решение «Шарады» 37. Квантовая криптография - основанная на принципах квантовой физики. Квантовый протокол распределения ключей. Распределение ключей в оптических сетях. 38. Криптографические протоколы: обеспечение различных режимов аутентификации; генерация, распределение и согласование криптографических ключей; защита взаимодействий участников; разделение ответственности между участниками. 39. Доказательство принадлежности (Zero-knowledge proof). Доказательство при отказе отправителя. Доказательство при отказе получателя. 40. Нормативно-правовое обеспечение информационной безопасности. 41. Классификация секретной информации в России. Служебная, коммерческая и государственная тайны. 42. Законы РФ: «Информации, информатизации и защите информации»; Закон о персональных данных

43. Стандарты ИБ: ISO/IEC 15408; руководящие документы ФСТЭК; Оранжевая книга (Критерии определения безопасности компьютерных систем - Trusted Computer System Evaluation Criteria; Радужная серия). 44. Политика безопасности. Уровень гарантированности. Классы безопасности. Безопасность распределенных систем. Рекомендации X.800. 45. Роли и ответственности субъектов информационного пространства. Принцип распределения ответственности. Матрица распределения доступа для сотрудников организации. 24 46. Понятие управления рисками. Качественные и количественные методики оценки рисков. Количественная модель рисков QRM (Quantitative Risk Model). Оценки по конфиденциальности информации. 47. Политика информационной безопасности. Цели и задачи организации. Взаимодействие между субъектами. Правила безопасности. 48. Политика информационной безопасности для локальной вычислительной сети. 49. Место криптографии в защите информации. Физическая защита. Стеганография. Криптография. 50. Предмет криптографии. Математические основы. 51. История криптографии. Шифр Цезаря. Считала. Маршрутная перестановка. Квадрат Полибия. 52. История криптографии. Магический квадрат. Таблица Тритемия. Решетка Кардано. 53. История криптографии. Шифр Виженера. Шифр Плейфера. Принцип Керкгоффа. 54. История криптографии. Лента Вернама. Энигма. 55. Математические основы криптографии. «Теория связи в секретных системах» Шеннона: математическая структура секретных систем. 56. Математические основы криптографии. «Теория связи в секретных системах» Шеннона: теоретическая секретность. 57. Математические основы криптографии. «Теория связи в секретных системах» Шеннона: практическая секретность. 58. Физические носители кодов паролей. 59. Требования к специализированным средствам защиты информации от несанкционированного доступа. 60. Организация виртуальных логических дисков 61. Одноуровневая модель разграничения доступа, достоинства и недостатки. 62. Многоуровневая модель разграничения доступа, достоинства и недостатки. 63. Применение специализированных программных средств защиты информации, их достоинства и недостатки

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	целенаправленная работа с информацией для использования в практических целях	Технология формирования уверенности и готовности к самостоятельной успешной профессиональной деятельности	ПК-4	З-1 З-2 У-1 П-1	Практические/семинарские занятия Экзамен