ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
ПО ДИСЦИПЛИНЕ

Основы управления информационной безопасностью

Код модуля	Модуль
1163595(1)	Основы управления информационной безопасностью

Екатеринбург

Оценочные материалы составлены автором(ами):

№ п/п	Фамилия, имя, отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Поршнев Сергей Владимирович	доктор технических наук, профессор	Профессор	Учебно-научный центр ”Информационная безопасность”
2	Сапронова Ольга Евгеньевна	без ученой степени, без ученого звания	Старший преподаватель	Учебно-научный центр ”Информационная безопасность”

Согласовано:

Управление образовательных программ Т.Г. Комарова

Авторы:

- **Поршнев Сергей Владимирович, Профессор, Учебно-научный центр "Информационная безопасность"**
- **Сапронова Ольга Евгеньевна, Старший преподаватель, Учебно-научный центр "Информационная безопасность"**

1. СТРУКТУРА И ОБЪЕМ ДИСЦИПЛИНЫ Основы управления информационной безопасностью

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

2. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ (ИНДИКАТОРЫ) ПО ДИСЦИПЛИНЕ МОДУЛЯ Основы управления информационной безопасностью

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 при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской	З-1 - Различать правовые и организационные меры защиты информации, в том числе информации ограниченного доступа З-2 - Изложить содержание нормативных правовых актов, нормативных и методических документов уполномоченных федеральных органов исполнительной власти (в том числе Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и	Домашняя работа Зачет Контрольная работа Лекции Практические/семинарские занятия

Федерации, Федеральной службы по техническому и экспортному контролю	экспортному контролю) по защите информации П-1 - Осуществлять обоснованный выбор нормативной базы в области защиты информации ограниченного доступа У-1 - Формулировать организационно-распорядительные документы, регламентирующие защиту информации ограниченного доступа в автоматизированных системах	
ПК-8 -Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	З-1 - Идентифицировать классификацию систем основные законы и закономерности систем информационной безопасности П-1 - Разрабатывать методики системного анализа У-1 - Выделять систему из внешней среды информационной безопасности	Домашняя работа Зачет Контрольная работа Лекции Практические/семинарские занятия
ПК-10 -Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма	З-1 - Описать основные закономерности исторического процесса, этапы исторического развития России, место и роль России в истории человечества и в современном мире П-1 - Иметь практический опыт выбора принципов историзма и научной объективности как основой формирования собственной гражданской позиции и развития патриотизма У-1 - Формулировать и аргументировано отстаивать собственную позицию по различным проблемам истории России	Домашняя работа Зачет Контрольная работа Лекции Практические/семинарские занятия

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 – 0.4		
Текущая аттестация на лекциях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
контрольная работа	6,12	*100*
Весовой коэффициент значимости результатов текущей аттестации по лекциям – 0.5		
Промежуточная аттестация по лекциям – зачет **Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – 0.5**		
2. Практические/семинарские занятия: коэффициент значимости совокупных результатов практических/семинарских занятий – 0.6		
Текущая аттестация на практических/семинарских занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
домашняя работа	6,6	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. Информационная безопасность и уровни ее обеспечения. Понятие "информационная безопасность". Проблема информационной безопасности общества. Определение понятия "информационная безопасность"

2. Составляющие информационной безопасности. Доступность информации. Целостность информации. Конфиденциальность информации

3. Система формирования режима информационной безопасности. Введение. Задачи информационной безопасности общества. Уровни формирования режима информационной безопасности

4. Уровни формирования режима информационной безопасности в РФ. Введение. Правовые основы информационной безопасности общества. Основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации. Ответственность за нарушения в сфере информационной безопасности. Выводы по теме

5. Стандарты информационной безопасности: "Общие критерии". Введение. Требования безопасности к информационным системам. Принцип иерархии: класс – семейство – компонент – элемент. Функциональные требования. Требования доверия. Выводы по теме

6. Стандарты информационной безопасности распределенных систем. Введение. Сервисы безопасности в вычислительных сетях. Механизмы безопасности. Администрирование средств безопасности. Выводы по теме

7. Стандарты информационной безопасности в РФ. Введение. Гостехкомиссия и ее роль в обеспечении информационной безопасности в РФ. Документы по оценке защищенности автоматизированных систем в РФ. Выводы по теме

8. Административный уровень обеспечения информационной безопасности. Введение. Цели, задачи и содержание административного уровня. Разработка политики информационной безопасности. Выводы по теме

9. Классификация угроз "информационной безопасности". Введение. Классы угроз информационной безопасности. Каналы несанкционированного доступа к информации. Выводы по теме

10. Компьютерные вирусы и защита от них. Вирусы как угроза информационной безопасности. Введение. Компьютерные вирусы и информационная безопасность. Характерные черты компьютерных вирусов. Выводы по теме. Расширяющий блок

11. Классификация компьютерных вирусов. Введение. Классификация компьютерных вирусов по среде обитания. Классификация компьютерных вирусов по особенностям алгоритма работы. Классификация компьютерных вирусов по деструктивные возможностям. Выводы по теме

12. Характеристика "вирусоподобных" программ. Введение. Виды "вирусоподобных" программ. Характеристика "вирусоподобных" программ. Выводы по теме.

13. Антивирусные программы. Введение. Особенности работы антивирусных программ. Классификация антивирусных программ. Факторы, определяющие качество антивирусных программ. Выводы по теме.

14. Профилактика компьютерных вирусов. Введение. Характеристика путей проникновения вирусов в компьютеры. Правила защиты от компьютерных вирусов. Выводы по теме.

15. Обнаружение неизвестного вируса. Введение. Обнаружение загрузочного вируса. Обнаружение резидентного вируса. Обнаружение макровируса. Общий алгоритм обнаружения вируса. Выводы по теме.

16. Механизмы обеспечения "информационной безопасности". Идентификация и аутентификация. Введение. Определение понятий "идентификация" и "аутентификация". Механизм идентификация и аутентификация пользователей. Выводы по теме.

17. Криптография и шифрование. Введение. Структура криптосистемы. Классификация систем шифрования данных. Симметричные и асимметричные методы шифрования. Механизм электронной цифровой подписи. Выводы по теме.

18. Методы разграничение доступа. Введение. Методы разграничения доступа. Мандатное и дискретное управление доступом. Выводы по теме

19. Регистрация и аудит. Введение. Определение и содержание регистрации и аудита информационных систем. Этапы регистрации и методы аудита событий информационной системы. Выводы по теме.

20. Межсетевое экранирование. Введение. Классификация межсетевых экранов. Характеристика межсетевых экранов. Выводы по теме.

21. Технология виртуальных частных сетей (VPN). Введение. Сущность и содержание технологии виртуальных частных сетей. Понятие "туннеля" при передаче данных в сетях. Выводы по теме.

22. Безопасность информационных систем. Безопасность UNIX

Примерные задания

Бывший сотрудник химико-биологического предприятия вместе со своим приятелем-программистом скопировали конфиденциальную информацию: состав ингредиентов, их пропорции и формулу нового лекарственного препарата – с целью продажи этой информации конкурирующей организации. Можно ли квалифицировать действия лица (группы лиц) в описанной ситуации как противоправные?

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. Преступления в сфере компью-терной информации

Примерные задания

Задачи, в которых необходимо спрогнозировать исход на основе описания жизненной ситуации, связанной с нарушением информационной безопасности.

Задачи по основным положениям главы 28 «Преступления в сфере компью-терной информации» Уголовного кодекса РФ.

Решение в пользу какой стороны и почему вынесет суд при предъявлении владельцем фирмы «Электронная галерея» И. С. Дубцовым судебного иска к продавцу этой же фирмы, если по вине последнего произошло электрическое замыкание и было повреждено

значительное количество компьютерной техники?

LMS-платформа − не предусмотрена

5.2.2. Домашняя работа

Примерный перечень тем

1. Преступления в сфере компью-терной информации

Примерные задания

Задачи, ориентированные на выявление каких-либо несоответствий, связанных с нарушением информационной безопасности. Задачи по основным положениям

главы 28 «Преступления в сфере компью-терной информации» Уголовного кодекса РФ.

По вине оператора по набору данных М. Л. Плехановой, работавшей с компьютерной системой бухгалтерских платежей, торговая сеть «Антиквар» понесла д нежные убытки в

размере 1 850 000 рублей. М. Е. Плехановой было предъявлено обвинение по ст. 273 УК

РФ.

LMS-платформа − не предусмотрена

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

5.3.1. Зачет

Список примерных вопросов

1. Основные понятия информационной безопасности.
2. Информационные технологии и необходимость ИБ.
3. Система защиты информации и ее структуры.
4. Экономическая информация как товар и объект безопасности.
5. Профессиональные тайны, их виды. Объекты коммерческой тайны на предприятии.
6. Персональные данные и их защита.
7. Информационные угрозы, их виды и причины возникновения.
8. Информационные угрозы для государства.
9. Информационные угрозы для компании.
10. Информационные угрозы для личности (физического лица).
11. Действия и события, нарушающие информационную безопасность.
12. Личностно-профессиональные характеристики и действия сотрудников, способствующих реализации информационных угроз.
13. Способы воздействия информационных угроз на объекты.
14. Внешние и внутренние субъекты информационных угроз.
15. Компьютерные преступления и их классификация.
16. Исторические аспекты компьютерных преступлений и современность.
17. Субъекты и причины совершения компьютерных преступлений.
18. Вредоносные программы, их виды.
19. История компьютерных вирусов и современность.
20. Деятельность международных организаций в сфере информационной безопасности.
21. Государственное регулирование информационной безопасности в РФ.
22. Задачи ИБ в программе « цифровая экономика».
23. Доктрина информационной безопасности России.
24. Федеральные законы в сфере информатизации и информационной безопасности в РФ.
25. Уголовно-правовой контроль над компьютерной преступностью в РФ.
26. Политика безопасности и ее принципы.
27. Фрагментарный и системный подход к защите информации.
28. Методы и средства защиты информации.
29. Организационное обеспечение ИБ.

30. Организация конфиденциального делопроизводства.
31. Организационно-экономическое обеспечение ИБ.
32. Инженерно-техническое обеспечение компьютерной безопасности.
33. Инженерно-техническое обеспечение компьютерной безопасности.
34. Защита информации в Интернете.
35. Электронная почта и ее защита.
36. Защита от компьютерных вирусов.
37. «Больные» мобильники и их «лечение».
38. Популярные антивирусные программы и их классификация.
39. Этапы и освоение защиты информации экономических объектов.
40. Криптографические методы защиты информации.
41. Оценка эффективности инвестиций в информационную безопасность.
42. Российские компании в сфере ИБ.
43. Фирмы, оценивающие работу персонала в компании.
44. Менеджмент и аудит ИБ на уровне предприятия.
45. Аудит ИБ автоматизированных банковских систем.
46. Аудит ИБ электронной коммерции.
47. Информационная безопасность предпринимательской деятельности

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	П-1	Домашняя работа Зачет Контрольная работа Лекции Практические/семинарские занятия