

**ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
ПО ДИСЦИПЛИНЕ**

Информационные технологии в области защиты информации

Код модуля
1156863(1)

Модуль
Информационные технологии

Екатеринбург

Оценочные материалы составлены автором(ами):

№ п/п	Фамилия, имя, отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Куц Дмитрий Владимирович	без ученой степени, без ученого звания	Старший преподаватель	Учебно-научный центр "Информационная безопасность"
2	Пономарева Ольга Алексеевна	кандидат технических наук, без ученого звания	Доцент	Учебно-научный центр "Информационная безопасность"
3	Поршнева Сергей Владимирович	д.т.н., профессор	директор Учебно-научного центра "Информационная безопасность"	УНЦ ИБ

Согласовано:

Управление образовательных программ

Т.Г. Комарова

Авторы:

- Куц Дмитрий Владимирович, Старший преподаватель,
- Пономарева Ольга Алексеевна, Доцент,
- Поршнев Сергей Владимирович, директор Учебно-научного центра "Информационная безопасность", УНЦ ИБ

1. СТРУКТУРА И ОБЪЕМ ДИСЦИПЛИНЫ Информационные технологии в области защиты информации

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 Информационные технологии в области 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
ОПК-2 -Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности	З-1 - Изложить состав, классификацию, особенности функционирования программных средств системного и прикладного назначений П-1 - Иметь навыки использования системного программного обеспечения для решения задач профессиональной деятельности П-2 - Иметь навыки использования прикладного программного обеспечения для	Домашняя работа Зачет Контрольная работа Лекции Практические/семинарские занятия

	<p>решения задач профессиональной деятельности</p> <p>У-1 - Рационально использовать функциональные возможности программных средств системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности</p>	
<p>ОПК-7 -Способен создавать программы на языках высокого уровня, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования</p>	<p>З-1 - Различать алгоритмические основы программирования на языках общего назначения</p> <p>З-2 - Различать языки программирования общего назначения</p> <p>П-1 - Иметь опыт разработки алгоритмов для последующего создания программ на языках общего назначения</p> <p>П-2 - Иметь опыт использования типовых инструментальных средств программирования для решения профессиональных задач</p> <p>У-1 - Формулировать способы организации программ и инструментария программирования при решении профессиональных задач</p>	<p>Домашняя работа</p> <p>Зачет</p> <p>Контрольная работа</p> <p>Лекции</p> <p>Практические/семинарские занятия</p>

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>	5,5	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 – 0.5		
Текущая аттестация на практических/семинарских занятиях	Сроки – семестр, учебная неделя	Максимальная оценка в баллах
<i>домашняя работа</i>	5,16	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. Изучение стандартных алгоритмов шифрования. Безопасность и быстрдействие криптосистем.
2. Изучение симметричных и ассиметричных криптосистем для защиты компьютерной информации.
3. Изучение принципов идентификации и механизмов подтверждения подлинности пользователя.
4. Правила формирования электронной подписи.
5. Изучение средств защиты локальных сетей от несанкционированного доступа.
6. Анализ функционирования маршрутизаторов, шлюзов сетевого уровня и межсетевых экранов.
7. Анализ способов защиты информации в компьютерных сетях от разрушающего программного воздействия.
8. Изучение требований по обеспечению информационной безопасности к аппаратным средствам и программному обеспечению.

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. Алгоритмы классической криптографии
2. Разграничение доступа, матрица доступа
3. Средства идентификации и аутентификации
4. Средства электронной подписи
5. Правила межсетевого экранирования

Примерные задания

Используя пропорциональный шифр, зашифровать:

1. информационная безопасность
2. автоматизированная система
3. шифрование

Используя шифр Виженера, зашифровать:

1. Исходный текст: гаммирование

Ключ: безопасность

2. Исходный текст: шифр

Ключ: ключ

Используя шифр двойной перестановки, зашифруйте:

Открытый текст: электронная подпись

Маршрут вписывания: слева - направо

Маршрут выписывания: сверху - вниз

Столбцы: (2, 3, 1, 4)

Строки: (2, 4, 1, 3, 5)

1. Дать характеристику понятиям: «метод доступа к объекту», «владелец объекта», «право доступа к объекту», «разграничение доступа».
2. Изучить и написать какие существуют модели разграничения доступа, дать характеристику каждой из них.
3. Изучить и написать какие существуют виды методов разграничения доступа, охарактеризовать каждый.
4. Дать характеристику понятию «VLAN».
5. Изучить и написать способы ограничения доступа к конкретным ресурсам (социальные сети, запрещенные сайты).
6. Написать список программ, обеспечивающих контроль и управление доступом в Интернет, защиту пользователей и сети предприятия, учет трафика, антивирусную защиту и контентную фильтрацию веб-трафика.
7. Написать как работает реализация запрета доступа к определенным объектам (система блокировок).

8. Изучить и написать какие существуют типы учетных записей управления компьютером, описать каждый тип

Расшифровать сообщения, зашифрованные методом Цезаря.

РЪАБА ШЮЙАП ОЩОСО БЬЕЦШТ ЩНРУЯ УЩЙГЦ ЯЩОРЫ ЙГТУА УЧЯЪБ
АЮНАТ УРЬЕШ ОЦЪОЩ
КЕЦШЫ ОТОЪШ БЬЮЩУ ЧЦЕУЮ АУЧЦХ РБЕЦА ЛАООТ ЯШОНЪ БХЙШО
ХОРИР ОУАБЫ ЙЩЙЧЯ
ЪЙЕЪШ ЯАЮОЖ ЫЙЧЕУ ЮАБГР ОАЦЦШ ОЮОЭБ ХЦШОЦ ЯАУШО УАЩЦМ
ШРУЪЫ ЙЧЯЪШ ЪОЩКЕ
ЦШЬЫЯ ЭОЯУА ЯНЪАЕ УЮЪЫС ЪСЫУР ОЪОЪЬ РУЩУ ЪПУЩЬ ЧЮБЩЦ
ЭЪЯЪБ АЮЦЪС ЪЫКЩЦ
ЭЮЦЩЦ ЦФОМА ЯНЯЩУ РОРЦТ ЦЖКВО ШУЩЙР ЦТЦЖК ТЙЪЩЦ ЛАБРУ
ЮЪБЪО ЪОШЬЮ ЪЩУРО
ТУРЬЕ ШООГЫ УАХОЕ УЪАЙТ ЮОХЫЦ ЖКЪУЫ НЛАЪО ТЯШОН ЯРЦАО
ШЬЮБЩ УРОАО ГЪТЦА
ЯЮУТК ПУЩЪС ЪТЫНР ЯНСЦЮ ЩНЫТО ЪЦЮЪХ ЭУЮУР ЦАОЦЖ ЩУЧВУ
УЪБЪЦ АЪУЕО ЪЦХРУ
ЫНРХТ ЙГОМЗ ЦГЮЙД ОЮУЧЯ РЦАОР ТЮБСЭ ОНДЭУ ЮУСЫБ ЩАНХО
ЮОЪЭБ ЦШЮЦЕ ЦАЭЪБ
ЪСЦАУ ЦЯАУШ ОМНЩЦ МШРУЫ ЫЙЪЯЪ ШЪЪХО ПЦЫАЪ РОБЪАЮ НЭЦДУ
ЧЫОСЬ ЩЪРУЪ БУЧШО
ЮАБЫЫ ЙЧЖЩУ ЪОРИОБ ШУТУЮ УРНЫЫ ЙЧЪУЕ ХОЭЩО ШОЩЦТ УРЬЕШ
ОЦЪОЩ КЕЦЩЦ ХОШЮЙ
ЩАНРУ ЯУЩЙЧ ПОЩОС ОЫЕЦШ

Расшифровать сообщения, зашифрованные методом Виженера.

ЯБЫСЪПОЦЪТЫТЗЮЫШЛЧВТРУЪЯЫУОДЪХКРЯОГХНЫРУЪСЪЦНУОТИНЫШТ
ЦЕЩАЧЫФОИЛКАФТТИЧГТПТЭКАЫШТЫОДЙЗЯЯБДУАЧТЮТЮПМЙВЪЫЙЫВЭО
СЕПТРЫВТЧОДХЮЧИБКПДСЧХЗНЪТХЙААЯПТИПЭЧВНЧЕЧЦСМИТХЯКЪЦЪДЫО
ПМЦЪДИЧЛМЪШЯЯФТЩОЪЕЧНХЫЩУОЩАФЭЯЪЦСЕЭТГЪЯЧННОЮЯЕЯЫЭУСТ
ТЭЕЯДЪХЧГЫДКЮГШУЗЪХМДХШЛНПАШПЦПЯПКЩЕЦМЦЫТХИРННЮСЫГЪН
БЪБНУОЯТКОЛХЧНВЪИМОЙХЦТТДОИФОЮЙЦОЦЪНАЪХШРЛШТЖШОКЯЕФУП
ПНЫВЫЧМУПЩЦОАУДЯСФЪМЭАТТДСХЙВЪХФЭЩЦИНАШШНСЯЫЪЧЕПЮПХ
ЪЧИЦОРАТХЫКТЧНЪЫЛХЭКУЩУЧАТХФЪЦХКЫШНЫЮЫФЧРЧНРЮРЙКСДТШЙ
БЫВЦОВЮЧУРЯЫЦФЪЧЫЦКВЫШЙДИХФЫГШФЛГЭЫЖАЮШПЙТЫМКРЯБУДСН
ШЗЪЯЫУОДЪХКРЯОГЧНЫВУЯЮШЯСТНШУОЯТЭШРЫЭУЧЯМЦЪООТТЪАЩЫБК
ХЪЦЧАНЦШОЩЪГЧСФМЧСЯЫКПВФРТПЫОФТЙЧЦЛЫВЫЙХЪЧИЪЦТЪШНБЪРЪТ
ХДКЮЫШЛЧКШАЖНАЪРЖТЫЩУЪЮПМЧБХЭЕШВЙМЙЖТСУЮЦЪННИЪИВЮГЪ
ИНЫРСКИЧТМЙЛДЯКГСЫЪЙКНЪЗЫХЕЩЫОШЙЛТЫКООТЮМЧЭСОРЯИЫЪТИЪ
ФИУИЯЫЧПЫШЪЧРЫЩЙЪРХЙКАБЕЯНЫЗНУЕНФЫЪШСЦИЧНФЪМГОДТПДЯ
НОХОЙЮПУХЖСИМРЫОТИЖЫТСТНЪНЦХШЩЫОТПЦЩУЦЪТНЪЕПЪТКЙЛЮМ

2. Электронная подпись

2.1. Сгенерируйте ключи RSA различной длины (напр., 1024 и 2048):

```
openssl genpkey -algorithm RSA -out key.pem -pkeyopt rsa_keygen_bits:2048
```

Посмотрите на структуру файла. Почему она такая?

2.2. Подпишите файлы разной длины разными ключами:

```
openssl rsautl -sign -in file -inkey key.pem -out sig
```

Как длина файла влияет на результат? Почему?

Как длина ключа влияет на результат? Почему?

2.3. Исследуйте блоки данных, формируемые для проверки подписи:

```
openssl rsautl -verify -in file -inkey key.pem -raw -hexdump
```

2.4. Проверьте подпись:

```
openssl rsautl -verify -in sig -inkey key.pem
```

Что произойдёт, если внести изменения в результат подписи? Попробуйте.

3. Совместное использование механизмов

3.1. Смоделируйте систему передачи между двумя сетевыми узлами, выбрав произвольные функции хеширования и подписи. Передайте зашифрованные любым алгоритмом файлы в обе стороны. Расшифруйте и проверьте подписи

LMS-платформа – не предусмотрена

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

5.3.1. Зачет

Список примерных вопросов

1. Государственная система защиты информации
2. Действия, относящиеся к мерам защиты информации.
3. Функции средств контроля доступа
4. Применение специальных программ для обнаружения попыток выполнить несанкционированные действия
5. Виды вредоносного ПО, их функциональные особенности
6. Виды специализированного ПО в области защиты информации
7. Криптографические средства защиты информации
8. Криптографические методы защиты информации
9. Симметричные алгоритмы шифрования
10. Асимметричные алгоритмы шифрования
11. Хеширование информации
12. Электронная подпись
13. Идентификация и аутентификация в компьютерных системах
14. Идентификация и аутентификация в ОС Linux
15. Идентификация и аутентификация в ОС Windows
16. Технологии защиты информации в компьютерных сетях
17. Виды межсетевое экранирования
18. Ограничение и разграничение доступа в компьютерных сетях
19. Алгоритмы классической криптографии

20. Противодействие вредоносному ПО

21. Антивирусные средства

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
Формирование информационной культуры в сети интернет	целенаправленная работа с информацией для использования в практических целях	Технология самостоятельной работы	ОПК-7	3-2	Домашняя работа Зачет Контрольная работа Лекции Практические/семинарские занятия