# ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ

Криптографические протоколы

**Код модуля**
1157393(1)

**Модуль**
Безопасность компьютерных систем

**Екатеринбург**

Оценочные материалы составлены автором(ами):

| № п/п | Фамилия, имя, отчество | Ученая степень, ученое звание | Должность | Подразделение |
|---|---|---|---|---|
| 1 | Агафонов Алексей Владимирович | кандидат технических наук, без ученого звания | Доцент | Учебно-научный центр "Информационная безопасность" |
| 2 | Пономарева Ольга Алексеевна | кандидат технических наук, без ученого звания | Доцент | Учебно-научный центр ”Информационная безопасность” |
| 3 | Поршнев Сергей Владимирович | д.т.н, профессор | директор Учебно-научного центра "Информационная безопасность" | УНЦ ИБ |
| 4 | Соколов Илья Петрович | без ученой степени, без ученого звания | Старший преподаватель | Учебно-научный центр ”Информационная безопасность” |

**Согласовано:**

Управление образовательных программ Т.Г. Комарова

**Авторы:**

- **Агафонов Алексей Владимирович, Доцент, Учебно-научный центр "Информационная безопасность"**
- **Пономарева Ольга Алексеевна, Доцент, Учебно-научный центр "Информационная безопасность"**
- **Поршнев Сергей Владимирович, директор Учебно-научного центра "Информационная безопасность", УНЦ ИБ**
- **Соколов Илья Петрович, Старший преподаватель, Учебно-научный центр "Информационная безопасность"**

## 1. СТРУКТУРА И ОБЪЕМ ДИСЦИПЛИНЫ Криптографические протоколы

| | | | |
|---|---|---|---|
| **1.** | **Объем дисциплины в зачетных единицах** | 3 | |
| **2.** | **Виды аудиторных занятий** | Лекции<br>Лабораторные занятия | |
| **3.** | **Промежуточная аттестация** | Экзамен | |
| **4.** | **Текущая аттестация** | Контрольная работа | 1 |
| | | Домашняя работа | 1 |

## 2. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ (ИНДИКАТОРЫ) ПО ДИСЦИПЛИНЕ МОДУЛЯ Криптографические протоколы

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-11 -Способен разрабатывать и реализовывать политики управления доступом в компьютерных системах | З-1 - Описать виды политик управления доступом и информационными потоками применительно к прикладному программному обеспечению<br>З-2 - Описать принципы функционирования программных средств криптографической защиты информации<br>З-3 - Описать виды политик управления доступом и | Домашняя работа<br>Контрольная работа<br>Лабораторные занятия<br>Лекции<br>Экзамен |

| | | |
|---|---|---|
| | информационными потоками в компьютерных сетях<br>П-1 - Определять порядок установки программного обеспечения с целью соблюдения требований по защите информации<br>П-2 - Контролировать соблюдение требований по защите информации при установке программного обеспечения, включая антивирусное программное обеспечение<br>П-3 - Выполнять разработку требований к параметрам средств антивирусной защиты для корректной работы программного обеспечения<br>У-1 - Формулировать политики безопасности операционных систем<br>У-2 - Настраивать политики безопасности операционных систем<br>У-3 - Проводить мониторинг функционирования программно-аппаратных средств защиты информации в компьютерных сетях | |

## 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 – 0.50** | | |
|---|---|---|
| **Текущая аттестация на лекциях** | **Сроки – семестр, учебная неделя** | **Максимальная оценка в баллах** |
| *контрольная работа* | *7,9* | *100* |
| **Весовой коэффициент значимости результатов текущей аттестации по лекциям – 0.50** | | |
| **Промежуточная аттестация по лекциям – экзамен**<br>**Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – 0.50** | | |

| | | |
|---|---|---|
| **2. Практические/семинарские занятия: коэффициент значимости совокупных результатов практических/семинарских занятий – не предусмотрено** | | |
| **Текущая аттестация на практических/семинарских занятиях** | **Сроки – семестр, учебная неделя** | **Максимальная оценка в баллах** |
| | | |
| **Весовой коэффициент значимости результатов текущей аттестации по практическим/семинарским занятиям– не предусмотрено** | | |
| **Промежуточная аттестация по практическим/семинарским занятиям–нет**<br>**Весовой коэффициент значимости результатов промежуточной аттестации по практическим/семинарским занятиям– не предусмотрено** | | |
| **3. Лабораторные занятия: коэффициент значимости совокупных результатов лабораторных занятий –0.50** | | |
| **Текущая аттестация на лабораторных занятиях** | **Сроки – семестр, учебная неделя** | **Максимальная оценка в баллах** |
| *домашняя работа* | 7,6 | 100 |
| **Весовой коэффициент значимости результатов текущей аттестации по лабораторным занятиям -1.00** | | |
| **Промежуточная аттестация по лабораторным занятиям –нет**<br>**Весовой коэффициент значимости результатов промежуточной аттестации по лабораторным занятиям – 0.00** | | |
| **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**<br>**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.<br>Студент способен выносить суждения, делать оценки и формулировать выводы в области изучения.<br>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. Лабораторные занятия

Примерный перечень тем

1. Производство и применение систем криптографической защиты информации
2. Функции органа криптографической защиты информации. Обязанности пользователей СКЗИ
3. Требования к средствам защиты информации используемым в криптопрооколах
4. Обязанности пользователей СКЗИ и криптопротоколов; Функции органа управления СКЗИ и использования криптопротоколов
5. Механизмы контроля за организацией и обеспечением безопасности хранения обработки и передачи конфиденциальных данных на основе криптопротоколов
6. Протоколы распределения ключей с центром доверия, основанные на симметричных криптосхемах: протокол Needham-Schroeder
7. Протоколы распределения ключей с центром доверия, основанные на симметричных криптосхемах: протокол протокол Kerberos
8. Протоколы транспортировки ключей, рекомендованные стандартом X.509, Протокол транспортировки ключей Beller-Yacobi
9. Протокол обмена ключами Диффи-Хеллмана, атаки на него
10. Протокол обмена ключами MTI, атаки на него
11. Протокол обмена ключами STS
12. Каналы защищенной передачи информации: постановка задачи, классификация средств обеспечения конфиденциальности и аутентичности
13. Протоколы распределения ключей с центром доверия, основанные на симметричных криптосхемах: протокол Otway-Rees
14. Доказательства с нулевым разглашением знаний. Алгоритмы разделения секрета

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. Криптографические протоколы

Примерные задания

1. Как преобразовать протокол аутентификации запрос-ответ на базе схемы открытого шифрования в протокол аутентичного распределения ключей? Приведите два примера: для протокола односторонней аутентификации и для протокола взаимной аутентификации.

2. Приведите описание процедуры восстановления секрета из схемы разделения секрета Шамира двумя способами: для случая, когда общее число участников равно 3, максимально допустимое количество утраченных (скомпроментированных) долей секрета равно 2, длина разделяемого секрета равно 128 битам.

LMS-платформа − не предусмотрена

**5.2.2. Домашняя работа**

Примерный перечень тем

1. Криптографические протоколы

Примерные задания

3. Какими из основных свойств протоколов распределения ключей (неявная аутентификация ключа, подтверждение ключа, явная аутентификация) обладает протокол Kerberos? Какие практические задачи он позволяет решать?

4. Оцените вычислительную сложность (количество выполненных операций) и коммуникационную сложность (количество пересылок сообщений и объем передаваемых данных) протокола доказательства знания дискретного логарифма для каждого участника. Приведите пример такого задания параметров протокола, при котором вероятность обмана доказывающим проверяющего не превысит $2^{-30}$.

5. Сравните по стойкости к различным видам атак два метода аутентификации по одноразовым паролям: метод Лэмпорта и последовательно обновляемые одноразовые пароли. Какие выводы о предпочтительности того или иного метода можно сделать?

LMS-платформа − не предусмотрена

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

**5.3.1. Экзамен**

Список примерных вопросов

1. Определение и свойства криптографических протоколов. Участники протокола. Общая классификация атак на криптографические протоколы. Компроментация криптографического протокола

2. Критерии оценки стойкости криптографических алгоритмов и протоколов

3. Характеристики вычислительно сложных задач теории чисел, возможности их применения в ассиметричной криптографии (задача факторизации и производные от нее задачи, задача дискретного логарифмирования и производные от нее задачи)

4. Парные отображения и их свойства. Вычислительно сложные задачи, основанные на парных отображениях

5. Основные подходы к конструированию стойких криптографических алгоритмов и протоколов в рамках концепции “доказательной безопасности”

6. Интерактивные системы доказательства: цель доказательства, общий принцип построения протокола, свойства полноты и корректности

7. Интерактивные системы доказательства с нулевым разглашением знания: цель доказательства, общий принцип построения протокола, свойство нулевого разглашения знания, теоремы

8. Классификация протоколов аутентификации. Атаки на протоколы с фиксированными паролями

9. Протоколы аутентификации с одноразовыми паролями. Схема Лэмпорта

10. Протоколы аутентификации “запрос-ответ”, основанные на симметричных криптосистемах: классификация, примеры, стандартизация (ISO/IEC 9798)

11. Протоколы аутентификации “запрос-ответ”, основанные на асимметричных криптосистемах: классификация, примеры, стандартизация (ISO/IEC 9798)

12. Протоколы аутентификации, основанные на доказательствах с нулевым разглашением знаний (на примере проокола Фиата-Шамира)

13. Общая классификация протоколов распределения ключей (ПРК), основные и дополнительные свойства ПРК

14. Классификация ПРК, основанных на симметричных криптосхемах. Двусторонние протоколы (без центра доверия)

15. ПРК с центром доверия, основанные на симметричных криптосхемах: протокол Needham-Schroeder, протокол Kerberos.

16. ПРК с центром доверия, основанные на симметричных криптосхемах: протокол OtwayRees, атаки на него

17. Классификация ПРК, основанных на симметричных криптосхемах. Протокол транспортировки ключей Needham-Schroeder с использованием схем открытого шифрования

18. Протоколы транспортировки ключей, рекомендованные стандартом X.509

19. Протокол транспортировки ключей Beller-Yacobi

20. Протокол обмена ключами Диффи-Хеллмана, атаки на него

21. Протокол обмена ключами MTI, атаки на него

22. Протокол обмена ключами STS

23. Каналы защищенной передачи информации: постановка задачи, классификация средств обеспечения конфиденциальности и аутентичности

24. Криптографические механизмы в спецификации SSH: аутентичное распределение ключей, защита передаваемых по каналу сообщений

25. Криптографические механизмы в спецификации SSL/TLS: аутентичное распределение ключей, защита передаваемых по каналу сообщений

26. Криптографические механизмы в спецификации IPSec: аутентичное распределение ключей, защита передаваемых по каналу сообщений

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 формирования уверенности и готовности к самостоятельной успешной профессиональной деятельности | ПК-11 | П-2 | Домашняя работа<br>Контрольная работа<br>Лабораторные занятия<br>Лекции<br>Экзамен |