КАЗАНСКИЙ КООПЕРАТИВНЫЙ ИНСТИТУТ (ФИЛИАЛ)
АВТОНОМНОЙ НЕКОММЕРЧЕСКОЙ ОБРАЗОВАТЕЛЬНОЙ
ОРГАНИЗАЦИИ ВЫСШЕГО ОБРАЗОВАНИЯ
ЦЕНТРОСОЮЗА РОССИЙСКОЙ ФЕДЕРАЦИИ
«РОССИЙСКИЙ УНИВЕРСИТЕТ КООПЕРАЦИИ»

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

МЕТОДЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Специальность: 10.05.01 Компьютерная безопасность
Специализация: «Разработка защищенного программного обеспечения»
Формы обучения: очная
Объем дисциплины:
в зачетных единицах: 9 з.е.
в академических часах: 324 ак.ч.

Форма промежуточной аттестации: экзамен

2025

Оценочные материалы по дисциплине Методы и средства криптографической защиты информации

обсуждены и рекомендованы к утверждению решением кафедры естественных дисциплин, сервиса и туризма от 25 марта 2025 г., протокол № 6

одобрены Научно-методическим советом Казанского кооперативного института (филиала) от 2 апреля 2025 г., протокол № 3

СОДЕРЖАНИЕ

Целью оценочных материалов по дисциплине (модулю) (далее –ОМ) является комплексная оценка результатов обучения по дисциплине Методы и средства криптографической защиты информации и установление уровня сформированности компетенций обучающегося.

ОМ предназначен для проведения текущего контроля успеваемости и промежуточной аттестации.

ОМ включает оценочные средства для проведения текущего контроля успеваемости и промежуточной аттестации.

Оценочные материалы разработаны в соответствии с рабочей программой дисциплины Методы и средства криптографической защиты информации.

1. Паспорт оценочных материалов по дисциплине «Методы и средства криптографической защиты информации»

Формируемые компетенции (код и наименование компетенции)	Индикаторы достижения компетенций	Планируемые результаты обучения	Контролируемые разделы, темы дисциплины	Наименование оценочного средства	
				Текущий контроль	Промежуточная аттестация
1	2	3	4	5	6
ОПК-10. Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ОПК-10.1. Применяет в профессиональной деятельности знания об основных алгоритмах, используемых в криптографии, а также методы оценивания сложности таких алгоритмов	Знать: основные алгоритмы, используемые в криптографии, их принципы работы и области применения, а также методы оценки их сложности и стойкости. Уметь: применять эти знания для анализа и выбора оптимальных алгоритмов в зависимости от конкретных задач и условий профессиональной деятельности. Владеть: навыками практического использования криптографических алгоритмов и методами их адаптации к различным информационным системам.	Тема 1 Виртуализация. Программные и аппаратные методы распределения ресурсов. Тема 2. Терминал и утилиты. CLI и методы работы с ним. Принципы работы терминала. Тема 7. Безопасность и работа с правами доступа к файловой системе и памяти.	Опрос (Тема 1-6) Доклад /Презентация (Тема 1-6) Тест (Тема 1-6)	Тест (П 1-4 тестового задания)

Формируемые компетенции (код и наименование компетенции)	Индикаторы достижения компетенций	Планируемые результаты обучения	Контролируемые разделы, темы дисциплины	Наименование оценочного средства	
				Текущий контроль	Промежуточная аттестация
1	2	3	4	5	6
	ОПК-10.3. Демонстрирует умения разработки криптографических протоколов и исследования их стойкости к различным атакам в составе средств защиты компьютерных систем	Знать: принципы разработки криптографических протоколов, включая их структуру, основные компоненты и методы обеспечения устойчивости к атакам. Уметь: разрабатывать криптографические протоколы, анализировать их эффективность и устойчивость к различным видам атак, а также адаптировать их под конкретные задачи защиты информации. Владеть: навыками исследования стойкости криптографических протоколов, тестирования их безопасности и применения на практике в составе комплексных средств защиты компьютерных систем.	Тема 3. Сетевой стек. Управление маршрутизацией. Тема 4. Сетевые службы. Системы доступа и хранения информации. Тема 8. Контейнеризация. Методы развертывание приложений посредством Docker.	Опрос (Тема 1-6) Доклад /Презентация (Тема 1-6) Тест (Тема 1-6)	Тест (П 5-9 тестового задания)

2. Оценочные материалы по дисциплине Методы и средства криптографической защиты информации

2.1 Оценочные материалы для проведения текущего контроля успеваемости

Тема 1. Встроенные средства обеспечения безопасности распространенных операционных систем и серверов различных сетевых протоколов.

Встроенные средства обеспечения безопасности распространенных операционных систем и серверов различных сетевых протоколов. Архитектура системы безопасности операционных систем.

Цель опроса – закрепить полученные знания и развить профессиональные навыки и умения, актуальные для будущих специалистов.

Критерии оценки:

«отлично» - ставится обучающемуся, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины и умение уверенно применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений;

«хорошо» - ставится обучающемуся, если он твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности;

«удовлетворительно» - ставится обучающемуся, показавшему фрагментарный, разрозненный характер знаний и может применять полученные знания по образцу в стандартной ситуации;

«неудовлетворительно» - ставится студенту, который не знает большей части основного содержания учебной программы дисциплины, допускает грубые ошибки в формулировках основных понятий дисциплины и не умеет использовать полученные знания при решении практических задач

Тематика докладов/презентаций:

1. Сравнительный анализ моделей управления доступом (DAC, MAC, RBAC) в ОС Windows и Linux.
2. Реализация централизованной аутентификации в доменной инфраструктуре Windows: Active Directory и Kerberos.
3. Встроенные механизмы защиты в ОС Linux: SELinux и AppArmor.
4. Защита сетевых сервисов с использованием TLS/SSL: принципы и реализация.
5. Архитектура подсистемы безопасности в Windows: LSASS, Security Accounts Manager (SAM), Local Security Policy.
6. Средства аудита и мониторинга безопасности в операционных системах.
7. Криптографические API в современных ОС: CryptoAPI (Windows), OpenSSL и GnuTLS (Linux).

8. Механизмы защиты от вредоносного ПО на уровне ОС: DEP, ASLR, SMEP и др.

Критерии оценки докладов:

– оценка *«отлично»* выставляется студенту, если выполнены все требования к написанию и защите доклада: обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объём, соблюдены требования к внешнему оформлению, даны правильные ответы на дополнительные вопросы.

– оценка *«хорошо»,* если основные требования к докладу и его защите выполнены, но при этом допущены недочёты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объём доклада; имеются упущения в оформлении; на дополнительные вопросы при защите даны неполные ответы.

– оценка *«удовлетворительно»,* если имеются существенные отступления от требований. В частности, тема освещена лишь частично; допущены фактические ошибки в содержании доклада или при ответе на дополнительные вопросы; во время защиты отсутствует вывод.

– оценка *«неудовлетворительно»* тема доклада не раскрыта, обнаруживается существенное непонимание проблемы.

Тесты по теме:

Какая модель управления доступом реализована по умолчанию в большинстве дистрибутивов Linux?

a) MAC
b) DAC
c) RBAC
d) ABAC

Какой компонент Windows отвечает за обработку запросов на аутентификацию и авторизацию?

a) Winlogon
b) LSASS
c) SAM
d) CSRSS

Какой из перечисленных модулей обеспечивает мандатный контроль доступа в ОС Linux?

a) AppArmor
b) PAM
c) SELinux
d) systemd

Какой протокол обеспечивает безопасную передачу данных в веб-серверах?

a) HTTP
b) FTP
c) HTTPS
d) SMTP

Какой механизм в ОС Windows защищает память от выполнения произвольного кода?

a) ASLR
b) UAC
c) DEP
d) TPM

Какая служба в Active Directory отвечает за выдачу билетов аутентификации?

a) LDAP
b) DNS
c) Kerberos
d) Group Policy

Какой стандарт лежит в основе большинства современных криптографических библиотек в Linux?

a) GOST
b) AES
c) OpenSSL
d) SHA-1

Какой из перечисленных компонентов НЕ входит в архитектуру подсистемы безопасности Windows?

a) Security Reference Monitor
b) Local Security Authority
c) NetBIOS
d) Security Accounts Manager

Критерии оценки тестов:
85% – 100% правильных ответов – «отлично»;
75% – 84% правильных ответов – «хорошо»;
50% – 75% правильных ответов – «удовлетворительно»;
менее 50 % правильных ответов – «неудовлетворительно».

Критерии оценки тестов:
85% – 100% правильных ответов – «отлично»;
75% – 84% правильных ответов – «хорошо»;
50% – 75% правильных ответов – «удовлетворительно»;
менее 50 % правильных ответов – «неудовлетворительно».

Тема 2. Основы криптографической защиты информации в компьютерных системах и сетях

Управление ключами. Время жизни ключей. Виды ключевой информации. Распределение ключей. Сертификация ключей. Причины ненадежности криптосистем. Человеческий фактор. Особенности реализации. Типичные ошибки пользователей. Применение нестойких криптоалгоритмов (КА). Неправильное применение КА. Ошибки в реализации КА. Криптография как математическая наука vs криптография как инженерная дисциплина

Цель опроса – закрепить полученные знания и развить профессиональные навыки и умения, актуальные для будущих специальстов.

Критерии оценки:

«отлично» - ставится обучающемуся, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины и умение уверенно применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений;

«хорошо» - ставится обучающемуся, если он твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности;

«удовлетворительно» - ставится обучающемуся, показавшему фрагментарный, разрозненный характер знаний и может применять полученные знания по образцу в стандартной ситуации;

«неудовлетворительно» - ставится студенту, который не знает большей части основного содержания учебной программы дисциплины, допускает грубые ошибки в формулировках основных понятий дисциплины и не умеет использовать полученные знания при решении практических задач

Тематика докладов/презентаций:

1. Инфраструктура открытых ключей (PKI): компоненты, принципы работы, уязвимости.
2. Сравнительный анализ устаревших и современных криптоалгоритмов: почему DES и MD5 больше не используются.
3. Человеческий фактор в криптографической безопасности: типичные ошибки пользователей и методы их минимизации.
4. Side-channel атаки: как реализация криптографии может быть уязвима даже при использовании стойких алгоритмов.
5. Проблемы управления ключами в распределённых системах и облачных средах.
6. Криптографические библиотеки с открытым исходным кодом: безопасность, надёжность, поддержка.
7. Различие между «доказуемой безопасностью» и «практической безопасностью» в криптографии.

8. Ошибки разработчиков при интеграции криптографии в приложения (на примере реальных уязвимостей: Heartbleed, ROCA и др.).

Критерии оценки докладов:

– оценка *«отлично»* выставляется студенту, если выполнены все требования к написанию и защите доклада: обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объём, соблюдены требования к внешнему оформлению, даны правильные ответы на дополнительные вопросы.

– оценка *«хорошо»,* если основные требования к докладу и его защите выполнены, но при этом допущены недочёты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объём доклада; имеются упущения в оформлении; на дополнительные вопросы при защите даны неполные ответы.

– оценка *«удовлетворительно»,* если имеются существенные отступления от требований. В частности, тема освещена лишь частично; допущены фактические ошибки в содержании доклада или при ответе на дополнительные вопросы; во время защиты отсутствует вывод.

– оценка *«неудовлетворительно»* тема доклада не раскрыта, обнаруживается существенное непонимание проблемы.

Тесты по теме:

Что из перечисленного НЕ относится к этапам жизненного цикла ключа?

a) Генерация
b) Распределение
c) Компиляция
d) Уничтожение

Какой тип ключа обычно используется для краткосрочного шифрования сессии?

a) Мастер-ключ
b) Сеансовый ключ
c) Открытый ключ
d) Хэш-ключ

Какая инфраструктура обеспечивает доверие к открытым ключам субъектов?

a) IPSec
b) PKI
c) TLS
d) SSH

Какой из перечисленных алгоритмов считается нестойким и не рекомендуется к использованию в новых системах?

a) AES-256

b) SHA-3

c) MD5

d) RSA-2048

Как называется уязвимость, возникающая из-за неправильного управления памятью в криптографической библиотеке OpenSSL?

a) Spectre

b) Heartbleed

c) Log4Shell

d) Meltdown

Какой из факторов чаще всего приводит к компрометации криптосистем на практике?

a) Математическая слабость алгоритма

b) Ошибки пользователей

c) Квантовые компьютеры

d) Аппаратные сбои

Что означает «side-channel атака»?

a) Атака на математическую модель алгоритма

b) Атака через утечку информации через физические параметры (время, энергопотребление и т.п.)

c) Атака на протокол передачи ключей

d) Атака через социальную инженерию

В чём основное различие между криптографией как наукой и как инженерной дисциплиной?

a) Научная криптография работает только с симметричными алгоритмами

b) Инженерная криптография учитывает ограничения реализации, удобство и совместимость

c) Научная криптография игнорирует вопросы производительности

d) Инженерная криптография не использует математические доказательства

Критерии оценки тестов:

85% – 100% правильных ответов – «отлично»;

75% – 84% правильных ответов – «хорошо»;

50% – 75% правильных ответов – «удовлетворительно»;

менее 50 % правильных ответов – «неудовлетворительно».

Тема 3. Продвинутые технологии криптографической защиты данных в компьютерных системах и сетях

Криптография как часть системы обеспечения безопасности информации (ОБИ). Философия проектирования систем ОБИ. Противоборствующее окружение. Параноидальная модель. Модель информационного противоборства. Информационная безопасность государства. Программные средства скрытого информационного воздействия (ПССИВ). Виды ПССИВ. Компьютерные вирусы (КВ).

Цель опроса – закрепить полученные знания и развить профессиональные навыки и умения, актуальные для будущих специальстов.

Критерии оценки:

«отлично» - ставится обучающемуся, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины и умение уверенно применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений;

«хорошо» - ставится обучающемуся, если он твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности;

«удовлетворительно» - ставится обучающемуся, показавшему фрагментарный, разрозненный характер знаний и может применять полученные знания по образцу в стандартной ситуации;

«неудовлетворительно» - ставится студенту, который не знает большей части основного содержания учебной программы дисциплины, допускает грубые ошибки в формулировках основных понятий дисциплины и не умеет использовать полученные знания при решении практических задач

Тематика докладов/презентаций:

1. Криптография как основа системы обеспечения безопасности информации
2. Философия проектирования систем обеспечения безопасности информации
3. Противоборствующее окружение в компьютерных системах и сетях
4. Параноидальная модель информационной безопасности
5. Модель информационного противоборства
6. Роль криптографии в информационной безопасности государства
7. Программные средства скрытого информационного воздействия: понятие и классификация
8. Виды программных средств скрытого информационного воздействия
9. Компьютерные вирусы: принципы работы и классификация
10. Криптографические методы сокрытия и защиты вредоносного ПО

Критерии оценки докладов:

– оценка *«отлично»* выставляется студенту, если выполнены все

требования к написанию и защите доклада: обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объём, соблюдены требования к внешнему оформлению, даны правильные ответы на дополнительные вопросы.

– оценка *«хорошо»,* если основные требования к докладу и его защите выполнены, но при этом допущены недочёты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объём доклада; имеются упущения в оформлении; на дополнительные вопросы при защите даны неполные ответы.

– оценка *«удовлетворительно»,* если имеются существенные отступления от требований. В частности, тема освещена лишь частично; допущены фактические ошибки в содержании доклада или при ответе на дополнительные вопросы; во время защиты отсутствует вывод.

– оценка *«неудовлетворительно»* тема доклада не раскрыта, обнаруживается существенное непонимание проблемы.

Тесты по теме:

Какую основную функцию выполняет криптография в системе ОБИ?

а) Повышение производительности системы

б) Обеспечение конфиденциальности, целостности и подлинности информации

в) Управление пользователями

г) Обнаружение аппаратных отказов

Что является ключевым принципом философии проектирования систем ОБИ?

а) Максимальное удобство пользователя

б) Минимизация затрат на разработку

в) Учет потенциального нарушителя

г) Отсутствие криптографических механизмов

Противоборствующее окружение — это:

а) Совокупность аппаратных средств

б) Среда эксплуатации системы без угроз

в) Совокупность факторов и субъектов, осуществляющих атаки

г) Пользовательский интерфейс системы

Параноидальная модель безопасности предполагает, что:

а) Нарушитель отсутствует

б) Нарушитель имеет ограниченные возможности

в) Любой элемент системы может быть скомпрометирован

г) Защита требуется только для критических данных

Что является целью модели информационного противоборства?
а) Увеличение скорости передачи данных
б) Получение, защита или искажение информации
в) Снижение энергопотребления системы
г) Оптимизация программного кода

Информационная безопасность государства в первую очередь направлена на:
а) Защиту персональных компьютеров граждан
б) Защиту коммерческой тайны предприятий
в) Защиту национальных информационных ресурсов и инфраструктуры
г) Развитие программного обеспечения

Программные средства скрытого информационного воздействия (ПССИВ) — это:
а) Легальное прикладное ПО
б) Программные средства защиты информации
в) ПО, скрытно воздействующее на информацию или систему
г) Диагностические утилиты

Какой признак характерен для ПССИВ?
а) Открытый исходный код
б) Явное уведомление пользователя
в) Скрытность функционирования
г) Высокая производительность

Компьютерный вирус — это:
а) Любая вредоносная программа
б) Программа, способная к самовоспроизведению
в) Средство сетевого администрирования
г) Аппаратный дефект системы

Зачем в вредоносном ПО используются криптографические методы?
а) Для ускорения работы программы
б) Для защиты пользователя
в) Для сокрытия кода и обхода средств обнаружения
г) Для резервного копирования данных

Критерии оценки тестов:
85% – 100% правильных ответов – «отлично»;
75% – 84% правильных ответов – «хорошо»;
50% – 75% правильных ответов – «удовлетворительно»;
менее 50 % правильных ответов – «неудовлетворительно».

Тема 4. Стохастические методы защиты информации

Основы теории генераторов псевдослучайных чисел(ГПСЧ). Требования к качественным ГПСЧ. Классификация ГПСЧ, ориентированных на использование в задачах криптографической защиты информации. Структура ГПСЧ. Типы используемых нелинейных функций. Блочные и поточные ГПСЧ.ГПСЧ на основе односторонних функций. ГПСЧ на регистрах сдвига с линейными и нелинейными обратными связями. ГПСЧ И.А. Кулакова. Основы теории конечных полей. Структура конечного поля. Мультипликативная группа конечного поля. Поля Галуа вида GF(p),где p– простое Поля Галуа вида GF(2n), где n–натуральное. Реализация операций сложения и умножения в конечных полях. Вычисление мультипликативной инверсии. ГПСЧ, функционирующие в конечных полях. Детальное описание раундов KAAES-128 и Кузнечик. Многомерные КА. Построение ранцевой криптосистемы на основе использования вычислений в конечных полях. Криптосистема Шора-Ривеста.

Цель опроса – закрепить полученные знания и развить профессиональные навыки и умения, актуальные для будущих специальстов.

Критерии оценки:

«отлично» - ставится обучающемуся, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины и умение уверенно применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений;

«хорошо» - ставится обучающемуся, если он твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности;

«удовлетворительно» - ставится обучающемуся, показавшему фрагментарный, разрозненный характер знаний и может применять полученные знания по образцу в стандартной ситуации;

«неудовлетворительно» - ставится студенту, который не знает большей части основного содержания учебной программы дисциплины, допускает грубые ошибки в формулировках основных понятий дисциплины и не умеет использовать полученные знания при решении практических задач

Тематика докладов/презентаций:

1. Основы теории генераторов псевдослучайных чисел (ГПСЧ)
2. Требования к качеству ГПСЧ в криптографических системах защиты информации
3. Классификация криптографически стойких генераторов псевдослучайных чисел
4. Структура ГПСЧ и типы используемых нелинейных функций
5. Блочные и поточные ГПСЧ: принципы построения и применения
6. ГПСЧ на основе односторонних функций и регистров сдвига с обратными связями
7. Основы теории конечных полей и поля Галуа GF(p) и GF(2^n)

8. Реализация операций сложения, умножения и вычисления мультипликативной инверсии в конечных полях
9. ГПСЧ, функционирующие в конечных полях, и их криптографические свойства
10. Использование вычислений в конечных полях в современных криптосистемах (AES-128, «Кузнечик», ранцевая криптосистема, Шора–Ривеста)

Критерии оценки докладов:

– оценка *«отлично»* выставляется студенту, если выполнены все требования к написанию и защите доклада: обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объём, соблюдены требования к внешнему оформлению, даны правильные ответы на дополнительные вопросы.

– оценка *«хорошо»,* если основные требования к докладу и его защите выполнены, но при этом допущены недочёты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объём доклада; имеются упущения в оформлении; на дополнительные вопросы при защите даны неполные ответы.

– оценка *«удовлетворительно»,* если имеются существенные отступления от требований. В частности, тема освещена лишь частично; допущены фактические ошибки в содержании доклада или при ответе на дополнительные вопросы; во время защиты отсутствует вывод.

– оценка *«неудовлетворительно»* тема доклада не раскрыта, обнаруживается существенное непонимание проблемы.

Тесты по теме:

Генератор псевдослучайных чисел (ГПСЧ) — это:

а) Истинный источник случайности

б) Алгоритм детерминированного формирования последовательности, имитирующей случайную

в) Аппаратный датчик шума

г) Средство шифрования данных

Основным требованием к криптографически стойкому ГПСЧ является:

а) Простота реализации

б) Высокая скорость работы

в) Непредсказуемость выходной последовательности

г) Минимальный размер кода

Какой признак отличает криптографический ГПСЧ от некриптографического?

а) Использование целых чисел
б) Устойчивость к восстановлению внутреннего состояния
в) Фиксированная длина периода
г) Использование линейных функций

Какая структура характерна для большинства ГПСЧ?

а) Таблица значений
б) Входной интерфейс пользователя
в) Внутреннее состояние и функция перехода
г) База данных

Для чего применяются нелинейные функции в ГПСЧ?

а) Для упрощения вычислений
б) Для увеличения статистической равномерности
в) Для повышения криптографической стойкости
г) Для сокращения периода

Регистры сдвига с линейной обратной связью (LFSR) характеризуются:

а) Криптографической стойкостью без доработок
б) Простотой реализации и линейностью
в) Абсолютной непредсказуемостью
г) Использованием односторонних функций

Конечное поле Галуа GF(p) определяется над:

а) Любым натуральным числом
б) Вещественными числами
в) Простым числом p
г) Чётным числом

Мультипликативная группа конечного поля состоит из:

а) Всех элементов поля
б) Только нулевого элемента
в) Всех ненулевых элементов поля
г) Только единицы

ГПСЧ, функционирующие в конечных полях, используют:

а) Только операции сложения
б) Арифметику конечных полей
в) Вещественные числа
г) Аппаратные генераторы шума

Вычисления в конечных полях используются в алгоритмах:

а) Сжатия данных

б) Контроля ошибок
в) Криптографических алгоритмах (AES, «Кузнечик»)
г) Графических интерфейсах

Критерии оценки тестов:
85% – 100% правильных ответов – «отлично»;
75% – 84% правильных ответов – «хорошо»;
50% – 75% правильных ответов – «удовлетворительно»;
менее 50 % правильных ответов – «неудовлетворительно».

Доклад – публичное сообщение на определенную тему, способствующее формированию навыков исследовательской работы, расширяющее познавательный интерес.

Работа над докладом состоит из следующих этапов:
- составление плана работы;
- систематизации полученных сведений;
- составление выводов и обобщений.

Доклад предоставляется в письменной форме.

Письменный доклад – это запись устного сообщения по какой-либо теме объёмом от пяти до пятнадцати страниц. В таком докладе не обязательно:
- выделять структурные элементы работы в виде плана;
- выделять заголовки внутри текста;
- ссылаться на использованную литературу по ходу текста.

Но обязательно следует приводить список всех используемых источников в конце работы. При подготовке доклада целесообразно соблюдать следующий порядок работы:

1. Подобрать литературу по изучаемой теме, познакомиться с её содержанием.
2. Пользуясь закладками, отметить наиболее существенные места или сделать выписки.
3. Составить план доклада.
4. Используя рекомендации по составлению тематического конспекта и составленный план, написать доклад, в заключение которого обязательно выразить своё отношение к излагаемой теме и её содержанию.
5. Прочитать текст и редактировать его.
6. Оформить в соответствии с требованиями к оформлению докладов

Тест – это система формализованных заданий, по результатам выполнения которых можно измерить уровень знаний, умений и навыков обучающегося.

2.2 Оценочные материалы для проведения промежуточной аттестации

Вопросы к экзамену:

ОПК-10.1. Применяет в профессиональной деятельности знания об основных алгоритмах, используемых в криптографии, а также методы оценивания сложности таких алгоритмов

1. Криптография в системе обеспечения безопасности информации цели задачи место в ОБИ
2. Философия проектирования систем обеспечения безопасности информации
3. Противоборствующее окружение и модели угроз
4. Параноидальная модель информационной безопасности
5. Модель информационного противоборства
6. Информационная безопасность государства и роль криптографических средств
7. Программные средства скрытого информационного воздействия понятие и классификация
8. Компьютерные вирусы принципы функционирования основные виды
9. Основы теории генераторов псевдослучайных чисел
10. Требования к качественным криптографическим ГПСЧ
11. Классификация ГПСЧ используемых в криптографической защите информации
12. Структура ГПСЧ и назначение нелинейных функций
13. Блочные и поточные ГПСЧ отличия и области применения
14. ГПСЧ на основе односторонних функций
15. Регистры сдвига с линейной и нелинейной обратной связью
16. ГПСЧ И А Кулакова
17. Основы теории конечных полей
18. Структура конечного поля
19. Мультипликативная группа конечного поля
20. Поля Галуа GF(p) где p простое
21. Поля Галуа GF(2n)
22. Операции сложения и умножения в конечных полях
23. Вычисление мультипликативной инверсии
24. ГПСЧ функционирующие в конечных полях
25. Криптографические автоматы и их классификация
26. Раунды алгоритма AES 128
27. Структура и раунды алгоритма Кузнечик
28. Многомерные криптографические автоматы
29. Ранцевая криптосистема на основе конечных полей
30. Криптосистема Шора Ривеста

ОПК-10.3. Демонстрирует умения разработки криптографических протоколов и исследования их стойкости к различным атакам в составе средств защиты компьютерных систем

1. Криптографическая стойкость и период псевдослучайной последовательности
2. Инициализация ГПСЧ и роль начального состояния
3. Статистические тесты качества псевдослучайных последовательностей
4. Атаки на генераторы псевдослучайных чисел
5. Криптографическая стойкость генераторов на регистрах сдвига
6. Использование нелинейных булевых функций в ГПСЧ
7. Представление элементов полей Галуа в полиномиальном виде
8. Использование конечных полей в блочных шифрах
9. Методы повышения стойкости криптографических автоматов
10. Ограничения и уязвимости стохастических методов защиты информации

Тестовые задания для проведения промежуточной аттестации.

Какие протоколы относятся к транспортному уровню четырехуровневой модели стека протоколов TCP/IP?
a. ARP
b. TCP
c. UDP
d. IP
e. ICMP

Виртуальные частные сети:
a. Передают частные данные по выделенным сетям
b. Инкапсулируют частные сообщения и передают их по общественной сети
c. Не используются клиентами Windows
d. Могут использоваться с протоколами L2TP или PPTP

Основные отличия протоколов L2TP и PPTP состоят в следующем (выберите все возможные варианты):
a. Протокол L2TP обеспечивает не конфиденциальность, а только туннелирование
b. Протокол PPTP используется только для туннелирования TCP/IP
c. Протокол L2TP может использоваться со службами IPSec, а протокол PPTP используется самостоятельно
d. Протокол PPTP поддерживается крупнейшими производителями, а протокол L2TP является стандартом корпорации Microsoft

Служба, осуществляющая присвоение реальных IP-адресов узлам закрытой приватной сети, называется:
a. NAT
b. PAT
c. Proxy
d. DHCP
e. DNS

На каком из четырех уровней модели стека протоколов TCP/IP к передаваемой информации добавляется заголовок, содержащий поле TTL (time-to-live)?
a. На уровне приложений (application layer)
b. На транспортном уровне (transport layer)
c. На сетевом уровне (internet layer)
d. На канальном уровне (link layer)

На каком уровне четырехуровневой модели стека протоколов TCP/IP работает служба DNS?
a. На уровне приложений (application layer)
b. На транспортном уровне (transport layer)
c. На межсетевом уровне (internet layer)
d. На канальном уровне (link layer)

Какой транспортный протокол используется протоколом Simple Mail Transfer Protocol (SMTP)?
a. TCP
b. UDP
c. ICMP
d. Ни один из перечисленных

Назовите отличия концентраторов (hub) от коммутаторов 2-го уровня (switch).
a. Коммутаторы работают на более высоком уровне модели OSI, чем концентраторы
b. Коммутаторы не могут усиливать сигнал, в отличие от концентраторов
c. Коммутаторы избирательно ретранслируют широковещательные кадры, концентраторы передают широковещательные кадры на все свои порты
d. Коммутаторы анализируют IP-адреса во входящем пакете, а концентраторы анализируют MAC-адреса

Какой из перечисленных компонентов НЕ входит в архитектуру подсистемы безопасности Windows?
a. Security Reference Monitor

b. Local Security Authority
c. NetBIOS
d. Security Accounts Manager

Выберите верное утверждение:
a. Протокол L2TP не имеет встроенных механизмов защиты информации
b. Протокол L2TP не применяется при создании VPN
c. Протокол PPTP более функциональный и гибкий чем L2TP, но требует более сложных настроек
Какой протокол служит, в основном, для передачи мультимедийных данных, где важнее своевременность, а не надежность доставки?
a. TCP
b. UDP
c. TCP, UDP

Протокол передачи команд и сообщений об ошибках:
a. ICMP
b. SMTP
c. TCP

С помощью какой команды можно просмотреть таблицу маршрутизации?
a. Route
b. Ping
c. Tracert

Какой из перечисленных алгоритмов считается нестойким и не рекомендуется к использованию в новых системах?
a. AES-256
b. SHA-3
c. MD5
d. RSA-2048

Что из перечисленного НЕ относится к этапам жизненного цикла криптографического ключа?
a. Генерация
b. Распределение
c. Компиляция
d. Уничтожение

Критерии оценки для проведения промежуточной аттестации по дисциплине (тестирование)

Шкала оценивания результатов промежуточной аттестации и критерии выставления оценок.

Оценка	**Уровень сформированности компетенции**	**Критерии**
«Отлично» («зачтено»)	Высокий	Выполнено более 80% заданий предложенного теста
«Хорошо» («зачтено»)	Хороший	Выполнено 60-80% заданий предложенного теста
«Удовлетворительно» («зачтено»)	Достаточный	Выполнено 35-60% заданий предложенного теста
«Неудовлетворительно» («не зачтено»)	Недостаточный	Выполнено менее 35% заданий предложенного теста

Обновление оценочных материалов дисциплины

обсуждено и рекомендовано к утверждению решением кафедры наименование кафедры
от ___ _____ 20_ г., протокол № ___

одобрено Научно-методическим советом _____ от ___ _____ 20__ г., протокол №____