МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ГЕОДЕЗИИ И КАРТОГРАФИИ
(МИИГАиК)

Факультет геоинформатики и информационной безопасности
Кафедра информационно-измерительных систем

**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 5BFEE1D286E9C95A0C0D2C611E434BD5
Владелец: Степанченко Алексей Леонидович
Действителен: с 23.09.2026 по 17.12.2027

«УТВЕРЖДАЮ»
Проректор
А. Л. Степанченко
15 мая 2026 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ (МОДУЛЮ) «Б1.В.08 РЕАЛИЗАЦИЯ СПЕЦИФИКАЦИИ КРИПТОГРАФИЧЕСКИХ СООБЩЕНИЙ»

Уровень высшего образования: магистратура

Направление подготовки: 10.04.01 Информационная безопасность

Направленность (профиль) подготовки: Защита информации в геоинформационных системах и системах сбора пространственных данных

Квалификация (степень) выпускника: магистр

Форма обучения: очная

Год набора (приема на обучение): 2026

Срок получения образования: 2 года

Объем: в зачетных единицах: 4 з.е.
в академических часах: 144 ак.ч.

Москва, 2026

Разработчики:
Преподаватель кафедры Информационно-измерительных систем
Месенгисер Я. Я.

Фонд оценочных средств по дисциплине (модулю) составлен в соответствии с требованиями ФГОС ВО по направлению подготовки 10.04.01 Информационная безопасность, утвержденного приказом Минобрнауки от 26.11.2020 № 1455

Согласование и утверждение

№	Подразделение	Ответственное лицо	ФИО	Виза	Дата, протокол (при наличии)
1	факультет Геоинформатики и информационной безопасности	Председатель ученого совета факультета	Матерухин А. В.	Рассмотрено	05.11.2025, № 12-25

1. Планируемые результаты обучения, соотнесенные с планируемыми результатами освоения образовательной программы

ПК-3 Способен разрабатывать проектные решения по защите информации автоматизированных систем (в том числе в геоинформационных системах)

ПК-3.1 Классифицирует защищаемую информацию по видам тайны и степеням конфиденциальности

Знать:

ПК-3.1/Зн1 Нормативно-правовые документы в области защиты информации, определяющие виды тайн и устанавливающие степени конфиденциальности

ПК-3.1/Зн2 Методы безопасности веб-приложения от критических угроз безопасности

ПК-3.1/Зн3 Систему нормативных правовых актов, нормативных и методических документов в области информационной безопасности и защиты информации

Уметь:

ПК-3.1/Ум1 Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности

ПК-3.1/Ум2 Выявлять и устранять потенциальные угрозы безопасности в веб-приложениях

ПК-3.1/Ум3 Обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей

Владеть:

ПК-3.1/Нв1 Методами анализа и оценки информации на предмет ее соответствия критериям отнесения к различным видам тайны и степеням конфиденциальности

ПК-3.1/Нв2 Навыками по применению нормативных правовых актов, нормативных и методических документов, регламентирующие деятельность по защите информации

ПК-3.2 Определяет типы субъектов доступа и объектов доступа, являющихся объектами защиты

Знать:

ПК-3.2/Зн1 Нормативные и методические документые, регламентирующие классификацию субъектов и объектов доступа

ПК-3.2/Зн3 Методы атаки и различные методы предотвращения атак

ПК-3.2/Зн4 Форматы криптографических сообщений и стандарты их представления

Уметь:

ПК-3.2/Ум1 Определять объекты доступа, которые подлежат защите, на основании их функционального назначения и чувствительности информации

ПК-3.2/Ум2 Выполнять проверку цифровых подписей и других криптографических атрибутов сообщений

ПК-3.2/Ум3 Анализировать результаты верификации и выявлять случаи нарушения целостности или подлинности сообщения

Владеть:

ПК-3.2/Нв1 Навыками работы с системами управления доступом и средствами контроля доступа

ПК-3.2/Нв2 Навыками работы с криптографическими библиотеками и инструментами верификации

ПК-3.2/Нв3 Методиками обеспечения безопасности при обработке и верификации криптографических сообщений

ПК-3.3 Разрабатывает проекты нормативных документов, регламентирующих работу по защите информации

Знать:

ПК-3.3/Зн1 Регламенты работ по обеспечению информационной безопасности автоматизированных систем автоматизированных систем

ПК-3.3/Зн2 Программные, технические и методические средства информационных технологий

Уметь:

ПК-3.3/Ум1 Разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности распределенных информационных систем

ПК-3.3/Ум2 Развертывать веб-приложения в безопасной среде и поддерживать безопасность веб-приложений

ПК-3.3/Ум3 Осуществлять разработку и проектирование информационных систем в соответствии с поставленной задачей

Владеть:

ПК-3.3/Нв1 Навыками разработки проектов нормативных документов, регламентирующих работу по защите информации в организации

ПК-3.3/Нв2 Методами анализа и формализации информационных процессов объекта и связей между ними

ПК-3.4 Понимает принципы построения и функционирования современных локальных и глобальных компьютерных сетей и их компонентов (в том числе геоинформационных систем)

Знать:

ПК-3.4/Зн1 Принципы построения и функционирования, примеры реализации современных локальных и глобальных компьютерных сетей и их компонентов (в том числе геоинформационных систем)

ПК-3.4/Зн3 Технологии проектирования и построения защищенных информационных систем

ПК-3.4/Зн4 Особенности архитектуры распределённых информационных систем и роли системного программного обеспечения в них

Уметь:

ПК-3.4/Ум1 Анализировать и выбирать оптимальную топологию и архитектуру сети с учетом требований и условий эксплуатации

ПК-3.4/Ум2 Выполнять настройку системного программного обеспечения с учетом требований информационной безопасности

Владеть:

ПК-3.4/Нв1 Навыками проектирования и построения локальных и глобальных компьютерных сетей с использованием современных технологий и оборудования

ПК-3.4/Нв2 Навыками работы с системным программным обеспечением различных платформ в распределённых ИС

2. Показатели и критерии оценивания компетенций

Планируемые результаты освоения программы	Уровень овладения	Критерии оценивания (перечень сформированных ИДК/ЗУВ по уровням освоения)

ПК-3 Способен разрабатывать проектные решения по защите информации автоматизированных систем (в том числе в геоинформационных системах)	Повышенный	ИДК ПК-3.1 Классифицирует защищаемую информацию по видам тайны и степеням конфиденциальности Знать: ПК-3.1/Зн1 Нормативно-правовые документы в области защиты информации, определяющие виды тайн и устанавливающие степени конфиденциальности ПК-3.1/Зн2 Методы безопасности веб-приложения от критических угроз безопасности ПК-3.1/Зн3 Систему нормативных правовых актов, нормативных и методических документов в области информационной безопасности и защиты информации

3. Шкала оценивания

Оценка	Критерии оценивания (перечень сформированных ИДК/ЗУВ)
Отлично	ПК-3.1 Классифицирует защищаемую информацию по видам тайны и степеням конфиденциальности ПК-3.1/Зн1 Нормативно-правовые документы в области защиты информации, определяющие виды тайн и устанавливающие степени конфиденциальности ПК-3.1/Зн2 Методы безопасности веб-приложения от критических угроз безопасности ПК-3.1/Зн3 Систему нормативных правовых актов, нормативных и методических документов в области информационной безопасности и защиты информации
Неудовле-творительно	Результаты обучения не сформированы на достаточном уровне

4. Контрольные мероприятия по дисциплине

Вид контроля	Форма контроля/Оценочное средство
Текущий контроль	Практическая работа Тестирование
Промежуточная аттестация	Зачет с оценкой

№ п/п	Наименование раздела	Контролируемые ИДК	Вид контроля/ используемые оценочные материалы	
			Текущий	Промежут. аттестация
1	Инфраструктура открытых ключей. Компоненты, функции, и архитектуры построения УЦ.	ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4	Практическая работа Тестирование	Зачет с оценкой
2	Спецификации PKCS#10, PKCS#12 и X.509	ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4	Практическая работа Тестирование	Зачет с оценкой
3	Спецификации PKCS#7, CMS и CAdES	ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4	Практическая работа	Зачет с оценкой
4	Спецификации XMLDSIG и XAdES	ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4	Практическая работа	Зачет с оценкой

5	Спецификация PAdES	ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4	Практическая работа	Зачет с оценкой

5. Порядок проведения промежуточной аттестации

Порядок проведения промежуточной аттестации регламентируется локальными нормативными актами Университета:

- Положением о формах, периодичности, порядке текущего контроля успеваемости и промежуточной аттестации обучающихся по основным образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры в федеральном государственном бюджетном образовательном учреждении высшего образования «Московский государственный университет геодезии и картографии», п.6 «Организация и проведение промежуточной аттестации».
- Положением о порядке осуществления образовательного процесса, проведения текущего контроля успеваемости и промежуточной аттестации обучающихся с применением электронного обучения и дистанционных образовательных технологий в федеральном государственном бюджетном образовательном учреждении высшего образования «Московский государственный университет геодезии и картографии», п.8 «Проведение промежуточной аттестации с применением ЭО и ДОТ».

Промежуточная аттестация: Зачет с оценкой, 1 семестр.

Промежуточная аттестация по дисциплине проводится в форме «дифференцированный зачет». Конкретная форма проведения — компьютерное тестирование по теоретическому материалу или устное собеседование по вопросам билетов — утверждается кафедрой и доводится до сведения обучающихся не позднее чем за месяц до начала промежуточной аттестации. При компьютерном тестировании итоговый результат определяется как отношение количества набранных баллов к максимально возможному количеству баллов. При устном собеседовании билет включает вопросы из перечня вопросов; преподаватель вправе задать дополнительные и уточняющие вопросы.

Критерии оценивания при проведении промежуточной аттестации в форме компьютерного тестирования:

Зачет оценивается по пятибалльной шкале:

- зачтено с оценкой «отлично» выставляется, если обучающийся набрал 86–100 баллов и продемонстрировал системное и полное освоение содержания дисциплины; ответы правильные, обоснованные и терминологически точные;
- зачтено с оценкой «хорошо» выставляется обучающемуся, набравшему 71–85 баллов, в случае, если основное содержание освоено, но допущены отдельные неточности, не влияющие на общее понимание материала;
- зачтено с оценкой «удовлетворительно» выставляется обучающемуся, набравшему 56–70 баллов, если освоены базовые понятия и положения, но имеются существенные пробелы и ошибки;
- не зачтено («не удовлетворительно») – если обучающийся набрал 0–55 баллов, не освоен необходимый минимум содержания дисциплины; результаты обучения не достигнуты.

Критерии оценивания при проведении промежуточной аттестации в форме устного собеседования по билетам:

Зачет оценивается по пятибалльной шкале:

- зачтено с оценкой «отлично» выставляется, если обучающийся набрал 86–100 баллов и дал полные, правильные и логически последовательные ответы; терминология применяется корректно, приведены необходимые обоснования и примеры, дополнительные вопросы раскрыты;
- зачтено с оценкой «хорошо» выставляется обучающемуся, набравшему 71–85 баллов, если вопросы раскрыты правильно и достаточно полно, а отдельные неточности исправлены после уточняющих вопросов;

- зачтено с оценкой «удовлетворительно» выставляется обучающемуся, набравшему 56–70 баллов, если основные положения раскрыты фрагментарно, имеются существенные неточности, однако базовое понимание продемонстрировано;
- не зачтено («не удовлетворительно») – если обучающийся набрал 0–55 баллов, вопросы не раскрыты либо допущены принципиальные ошибки, отсутствует владение базовой терминологией.

6. Оценочные материалы текущего контроля

Раздел 1. Инфраструктура открытых ключей. Компоненты, функции, и архитектуры построения УЦ.

Контролируемые ИДК: ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4

Тема 1.1. Инфраструктура открытых ключей

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Правовые основания учебного обмена

Для обмена документами между двумя условными участниками определить применимые положения закона об электронной подписи, требуемый вид подписи и условия ее проверки. Отдельно указать, какие признаки нельзя подтвердить одним успешным запуском криптографической библиотеки.

2. Процесс проверки сообщения

Описать небольшой сервис приема и проверки подписанного документа: входы, этапы, результаты, отказ и ответственные компоненты. Сформулировать требования к сохранению исходных данных и понятному отчету с отдельными итогами криптографической проверки и доверия.

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Упорядочьте подготовку проверяемого требования к сервису проверки подписей.

А. Сформулировать условие и наблюдаемый критерий
Б. Определить данные и требуемый результат проверки
В. Подготовить учебный пример для проверки критерия

2. Упорядочьте правовое обоснование применения электронной подписи для заданного обмена.

А. Зафиксировать допустимый вид подписи и порядок проверки
Б. Определить вид документа и участников
В. Проверить применимые нормы и соглашения

Тема 1.2. Понятия удостоверяющего центра

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Учебные УЦ и кросс-сертификация

Построить схему двух учебных УЦ, обменяться запросами и выпустить кросс-сертификат для ключа другого УЦ с явно заданными полномочиями CA. Сравнить его с обычным сертификатом пользователя, указать якорь доверия и построить путь проверки; сопоставить схему с иерархией и мостовой PKI.

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Упорядочьте работу с путем сертификации, если доверенные основания уже определены политикой.

А. Выбрать применимый заранее доверенный якорь
Б. Проверить сертификаты и ограничения найденного пути

В. Найти связанный с ним путь к целевому сертификату

2. В учебной схеме сертификат пользователя выдан УЦ Б, а сертификат УЦ Б выдан УЦ А. Упорядочьте путь от доверенного УЦ А к пользователю.

А. Сертификат УЦ Б
Б. Сертификат пользователя
В. Доверенный УЦ А

Раздел 2. Спецификации PKCS#10, PKCS#12 и X.509

Контролируемые ИДК: ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4

Тема 2.1. Генерация ключевой пары

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Подготовка OpenSSL с ГОСТ и взаимная проверка подписей

Подготовить выданную учебную среду OpenSSL с GOST Engine: зафиксировать версии, зависимости и подмодули, проверить загрузку модуля. Собрать среду по инструкции либо проверить готовую сборку. Создать две учебные пары ГОСТ Р 34.10-2012, подписать короткие сообщения с ГОСТ Р 34.11-2012, обменяться только открытыми ключами, сообщениями и подписями; проверить исходный и измененный файлы. Сопоставить операции с вызовами Bouncy Castle.

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Упорядочьте создание новой учебной ключевой пары средствами библиотеки.

А. Сохранить закрытую часть с нужной защитой доступа
Б. Вызвать генерацию и проверить успешность
В. Выбрать поддерживаемый алгоритм и параметры по заданному профилю

2. Упорядочьте проверку вновь созданной учебной ключевой пары с помощью простого подписанного сообщения.

А. Проверить подпись соответствующим открытым ключом
Б. Зафиксировать результат проверки исходного сообщения
В. Создать подпись контрольного сообщения закрытым ключом

Тема 2.2. Импорт и экспорт ключевой пары

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Перенос ключевого материала

Экспортировать учебную пару в согласованном защищенном формате и импортировать в другую библиотеку или учебную среду. Сопоставить открытые части, проверить работу пары и отметить права доступа к файлам, парольному вводу и журналам.

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Упорядочьте перенос защищенного файла закрытого ключа в новую учебную среду.

А. Проверить соответствие импортированной пары ожидаемому открытому ключу
Б. Экспортировать ключ в согласованном защищенном представлении
В. Передать файл по разрешенному каналу и импортировать

2. Упорядочьте разбор текстового представления криптографического объекта.

А. Разобрать полученную структуру соответствующего типа
Б. Декодировать Base64 предусмотренным средством
В. Определить тип по границам и метке

Тема 2.3. Создание запроса на сертификат ключа проверки ЭП и получение сертификата ключа проверки ЭП

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. PKCS#10: поля ASN.1 и проверка подписи запроса

Сформировать запрос PKCS#10 с учебным именем, открытым ключом и запрошенными расширениями. Разобрать ASN.1, найти CertificationRequestInfo и подпись, определить их границы по фактической структуре файла. Проверить запрос штатной командой и сопоставить с проверкой выделенного DER-представления; повторить проверку после изменения подписанного поля.

2. Прием ответа удостоверяющего центра

Для нескольких учебных ответов сопоставить субъект, открытый ключ, издателя и назначение сертификата с исходной заявкой. Выявить сертификат с другим ключом и оформить обоснованное решение о его непригодности для данной пары.

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Упорядочьте создание запроса PKCS#10 для уже подготовленной ключевой пары.

А. Сформировать имя, открытый ключ и требуемые атрибуты
Б. Проверить полученный запрос и передать его в учебный УЦ
В. Подписать информацию запроса закрытым ключом заявителя

2. Упорядочьте прием сертификата в ответ на учебный запрос.

А. Получить выпущенный сертификат
Б. Проверить издателя, ограничения и применимость для задачи
В. Сопоставить его субъект и открытый ключ с ожидаемыми

Тема 2.4. Создание самоподписанного сертификата ключа проверки ЭП

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Самоподписанный X.509: структура и доверие

По учебному запросу создать самоподписанный сертификат, разобрать TBSCertificate, алгоритм и значение подписи. Проверить подпись над правильным DER-представлением и сравнить со штатной проверкой. Настроить отдельное учебное хранилище доверия и объяснить различие результатов до и после включения сертификата.

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Упорядочьте создание учебного самоподписанного сертификата при наличии ключа.

А. Прочитать поля и проверить подпись созданного сертификата
Б. Подписать сертификат соответствующим закрытым ключом
В. Задать имя, сроки и необходимые расширения

2. Упорядочьте включение учебного корневого сертификата в локальную политику доверия.

А. Добавить его в разрешенное хранилище доверия с учетом политики
Б. Получить сертификат и подтверждение его принадлежности по принятому каналу
В. Сверить проверяемые сведения с утвержденным основанием

Тема 2.5. Подпись запроса на сертификат ключа проверки ЭП

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Выдача сертификата и привязка подтверждения к заявке

Реализовать учебную выдачу сертификата по CSR с проверкой подписи, сведений заявителя и

допустимости расширений. В локальном макете разобрать случай: подтверждение относится только к открытому ключу, а запрашиваемые права между согласованием и выпуском меняются. Связать подтверждение с неизменным согласованным запросом и политикой прав, затем показать отказ для измененной заявки.

Тема 2.6. Создание, импорт и экспорт PFX

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Создание контейнера PFX

Собрать PKCS#12 из согласованных учебных ключа, сертификата и цепочки. Проверить состав объектов, защиту и возможность открытия с правильным паролем; сопоставить число сертификатов с числом ключей. Сопоставить контейнер с примером PKCS#12 в учебном репозитории; определить фактически поддерживаемую защиту ключа и целостности.

2. Импорт и диагностика PKCS#12

Перенести контейнер в другую учебную среду или разобрать предоставленные результаты двух библиотек. Проверить правильный и неверный пароль, соответствие ключа сертификату и права после импорта; объяснить, почему отключение проверки целостности не исправляет причину отказа. При использовании ГОСТ-ключей проверить совместимость конкретного профиля PFX; наличие поддержки подписи ГОСТ не считается доказательством поддержки любого ГОСТ-контейнера.

Раздел 3. Спецификации PKCS#7, CMS и CAdES

Контролируемые ИДК: ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4

Тема 3.1. Обзор спецификаций CAdES, PKCS#7 и CMS

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Присоединенная и отделенная CMS/CAdES-подпись

Подготовить короткий запрос ресурса в JSON и зафиксировать его точные байты. Средствами OpenSSL с GOST Engine сформировать в DER присоединенную и отделенную CMS-подписи, применив предусмотренные -cades атрибуты. Разобрать ASN.1, найти содержимое, SignerInfo и атрибуты. Проверить подпись и соответствие message-digest фактическим байтам JSON; передать локальному приложению только проверенное содержимое. Изменить запрос после подписания и показать отказ при проверке. Отдельно собрать и разобрать собственную ASN.1-последовательность из примера переписки: UTF8String с JSON и OCTET STRING с байтами подписи; объяснить отличие этой структуры от CMS, не предполагая совместимость с текущим ботом. Сравнить учебную проверку с -noverify и проверку сертификата по заданному хранилищу доверия. Передать открытые образцы в Base64 и проверить сохранение байтов после обратного преобразования.

2. Свидетельство времени и статус сертификата

По готовым учебным CAdES-примерам или собственному стенду сопоставить заявленное signing-time и токен независимой службы времени. Проверить привязку токена и разобрать результаты CRL/OCSP, не смешивая статус отзыва со сроком и общим доверием.

3. Профиль CAdES и регламент проверки

Для заданного сценария хранения определить нужные материалы проверки и описать различия B-B, B-T, B-LT и B-LTA. Подготовить проект регламента приемки сообщения с условиями положительного, отрицательного и неопределенного результата.

Раздел 4. Спецификации XMLDSIG и XAdES

Контролируемые ИДК: ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4

Тема 4.1. Обзор спецификаций XMLDSIG и XAdES

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Подпись XML и охват ссылок

Создать либо разобрать учебную XML-подпись средствами обработки XML с криптографической библиотекой. Найти SignedInfo, Reference и SignatureValue, установить подписанные объекты и проверить изменение текста одного из них.

2. Связь проверенного XML с действием приложения

Разобрать учебный документ с двумя одноименными узлами, из которых подписан только один. Исправить выбор данных приложением так, чтобы использовался проверенный объект; задать ограничения внешних ссылок и допустимых преобразований.

3. Свойства и уровень XAdES

В учебной XAdES-подписи определить SignedProperties, UnsignedProperties и ссылки на защищаемые свойства. Проверить состав заданного baseline-уровня и отделить результат разбора XML от криптографических и профильных проверок.

Раздел 5. Спецификация PAdES

Контролируемые ИДК: ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4

Тема 5.1. Обзор спецификации PAdES

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Диапазоны PDF-подписи

Создать или разобрать небольшой подписанный PDF специализированным средством формата с использованием криптографической библиотеки. Найти ByteRange и Contents, определить охваченную ревизию и сравнить изображение подписи с криптографической структурой.

2. Проверка нескольких ревизий PDF

Рассмотреть учебный PDF с последовательными подписями и добавленными материалами проверки. Для каждой подписи указать охват, результат проверки и допустимость последующих изменений по заданной политике.

3. Интеграция сервиса проверки форматов

Подготовить конфигурацию или небольшой прототип сервиса проверки учебных CMS/XML/PDF-образцов в доступной среде. Задать отдельное хранилище доверия, ограничения доступа к ключам и внешним источникам, форму отчета и правила обработки неопределенного статуса; отделить технический итог от правового признания.

7. Оценочные материалы промежуточной аттестации

1 семестр, Зачет с оценкой

Контролируемые ИДК: ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4

Вопросы/Задания:

1. Какие основные участники нужны для выдачи и проверки сертификата?

2. Чем правовой вид подписи отличается от формата криптографического контейнера?

3. Какую связь удостоверяет сертификат открытого ключа?

4. Почему перед внедрением электронной подписи уточняют условия обмена документами?

5. Какие результаты следует раздельно показывать в отчете проверяющего сервиса?

6. В чем особенность иерархической PKI?

7. Как кросс-сертификация связывает домены доверия?

8. Для чего применяется мостовой УЦ?

9. Почему построение пути не равно успешной проверке доверия?

10. Почему якорь доверия нельзя брать из любого присланного сообщения?

11. Что проверяют после подготовки OpenSSL с GOST Engine?

12. Какие разные роли выполняют ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012?

13. Почему открытый ключ можно распространять, а закрытый требует ограничения доступа?

14. Какие проверки полезны после создания пары?

15. Что учитывать при хранении учебного закрытого ключа?

16. Чем текстовое представление PEM отличается от шифрования ключа?

17. Что дает согласованный формат обмена закрытыми ключами?

18. Почему при импорте недостаточно ориентироваться на расширение файла?

19. Как проверить, что после переноса используется та же ключевая пара?

20. Почему пароль экспорта не следует включать в общий журнал команды?

21. Какие основные сведения входят в PKCS#10?

22. Что подтверждает правильная подпись запроса и чего она не подтверждает сама?

23. Почему ответ УЦ проверяют на соответствие открытому ключу запроса?

24. Какую роль выполняет ContentSigner при построении CSR в Bouncy Castle?

25. Почему при разборе CSR нельзя механически повторять offset и length из чужого журнала?

26. Чем самовыданный сертификат отличается от самоподписанного?

27. Над какой структурой создается подпись сертификата X.509?

28. Какие поля задают временную область действия сертификата?

29. Зачем задавать keyUsage и basicConstraints?

30. Какие результаты сравнивают при проверке сертификата до и после добавления учебного доверия?