Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Гриб Владислав Валерьевич
Должность: Ректор
Дата подписания: 06.11.2026 16:55:37
Уникальный программный ключ:
637517d24e103c3db032acf37e839d98ec1c5bb2f5eb89c29abfcd7f43985447

Образовательное частное учреждение высшего образования

«МОСКОВСКИЙ УНИВЕРСИТЕТ ИМЕНИ А.С. ГРИБОЕДОВА»

(ИМПЭ им. А.С. Грибоедова)

ФАКУЛЬТЕТ СРЕДНЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
(МЕЖДУНАРОДНЫЙ ДИПЛОМАТИЧЕСКИЙ КОЛЛЕДЖ)

УТВЕРЖДАЮ
Директор Международного
дипломатического колледжа
_____ Н.И. Платонова
«16» февраля 2026г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
по учебной дисциплине

Основы информационной безопасности

Специальность
09.02.11 Разработка и управление программным обеспечением

Квалификация выпускника:
Программист

на базе среднего общего образования

Форма обучения: очная

Москва

Фонд оценочных средств для дисциплины «Стандартизация, сертификация и техническое документоведение». Специальность 09.02.11 Разработка и управление программным обеспечением /– М.: ИМПЭ им. А. С. Грибоедова.

Фонд оценочных средств является неотъемлемой частью рабочей программы дисциплины.

Организация-разработчик: Образовательное частное учреждение высшего образования «Московский университет имени А. С. Грибоедова»

Директор Международного
дипломатического колледжа_____/Н.И. Платонова

1. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Настоящий Фонд оценочных средств (ФОС) по дисциплине «Стандартизация, сертификация и техническое документоведение» является неотъемлемым приложением к рабочей программе дисциплины (РПД) «Стандартизация, сертификация и техническое документоведение». На данный ФОС распространяются все реквизиты утверждения, представленные в РПД по данной дисциплине.

2. ПЕРЕЧЕНЬ ОЦЕНОЧНЫХ СРЕДСТВ

Для определения качества освоения обучающимися учебного материала по дисциплине используются следующие оценочные средства:

№ п/п	Оценочное средство	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС
1	Тестирование	Вид контроля, позволяющий оценить изученный теоретический материал.	Вопросы для проведения тестирования
2	Практические задания	Вид контроля, позволяющий оценить умение обучающегося применять осваиваемую компетенцию в практических ситуациях и при решении производственных задач	Задания к практическому занятию
3	Контрольная работа	Вид контроля, позволяющий определить результат освоения компетенций по дисциплине в рамках рассматриваемой темы, оцениваемый с помощью соответствующих индикаторов достижения компетенций	Задания контрольной работы
4	Самостоятельная работа	Вид контроля, позволяющий оценить проработку теоретического материала, изучение рекомендуемой литературы, выполнение практико-ориентированных заданий (заполнение таблиц, проведение сравнительного анализа, составление схем и др.), решение практических задач, создание презентаций, написание рефератов, подборку нормативного и иного материала и выполнение других заданий	Задания самостоятельной работы
5.	Зачет/Зачет с оценкой/Экзамен	Вид контроля, позволяющий выявить степень овладения знаниями, умениями и навыками, необходимыми для дальнейшего освоения образовательной программы подготовки	Вопросы для подготовки к зачету/зачету с оценкой/экзамену

3.ТИПОВЫЕ КОНТРОЛЬНЫЕ ЗАДАНИЯ ИЛИ ИНЫЕ МАТЕРИАЛЫ, НЕОБХОДИМЫЕ ДЛЯ ОЦЕНКИ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

Темы для подготовки к промежуточной аттестации

1. Основные понятия информационной безопасности. Триада CIA (конфиденциальность, целостность, доступность). Дополнительные свойства (аутентичность, неотказуемость). Классификация угроз и уязвимостей.
2. Нормативно-правовое регулирование в области ИБ в РФ. Федеральный закон №152ФЗ «О персональных данных»: основные принципы и требования. Федеральный закон №187-ФЗ «О безопасности КИИ»: ключевые понятия.
3. Основы криптографии. Симметричное и асимметричное шифрование: принципы работы, области применения, примеры алгоритмов (AES, RSA). Криптографические хэш-функции: свойства и применение (целостность, хранение паролей).
4. Вредоносное программное обеспечение (Malware). Классификация (вирусы, черви, трояны, ransomware). Основные каналы распространения и методы защиты на уровне пользователя и организации.
5. Основы сетевой безопасности. Базовые сетевые угрозы: спуфинг, сниффинг, DoS/DDoS-атаки. Назначение и принципы работы межсетевых экранов (firewall). Понятие VPN.
6. Модели управления доступом. Дискреционная (DAC), ролевая (RBAC) и мандатная (MAC) модели доступа. Сравнительный анализ, достоинства и недостатки. Принцип минимальных привилегий.
7. Основные угрозы безопасности баз данных. SQL-инъекция: механизм, виды, последствия. Общие методы защиты от несанкционированного доступа к данным.
8. Администрирование безопасности в СУБД. Задачи администратора БД по обеспечению безопасности. Управление пользователями, ролями и привилегиями. Понятие аудита (логирования) событий безопасности.
9. Технологии защиты данных в базах данных. Шифрование данных: прозрачное (TDE) и на уровне столбцов. Маскирование и анонимизация данных. Резервное копирование как элемент обеспечения доступности.
10. Безопасное программирование (Secure Coding). Обзор OWASP Top 10 (на примере SQLi, XSS, уязвимых компонентов). Основные принципы: валидация входных данных, экранирование выходных данных, использование параметризованных запросов.
11. Инструменты анализа защищенности ПО. Статический (SAST) и динамический (DAST) анализ: цели, принципы работы, отличия. Назначение баз уязвимостей (CVE/NVD) в процессе разработки.
12. Обеспечение безопасности в облачных средах. Модель общей ответственности (Shared Responsibility Model) в облачных сервисах. Ключевые аспекты безопасности баз данных, развернутых в облаке.
13. Эволюция понятия «информационная безопасность»: от защиты данных к кибербезопасности и управлению рисками.
14. Атаки на конфиденциальность: методы перехвата информации (сниффинг, социальная инженерия, утечки данных).

15. Атаки на целостность: способы несанкционированного изменения данных (подмена, манипуляция пакетами, атаки «человек посередине»).
16. Атаки на доступность: отказ в обслуживании (DoS/DDoS) – виды, принципы работы, цели атакующих.
17. Уязвимости нулевого дня (Zero-day): определение, жизненный цикл, экономика и значение для безопасности ПО.
18. Стандарт PCI DSS: основные требования к безопасности данных держателей платежных карт.
19. Концепция «Защита в глубину» (Defense in Depth): принципы многоуровневой защиты информационной системы.
20. Криптостойкость: факторы, влияющие на стойкость шифрования, понятие о полном переборе и атаках по сторонним каналам.
21. Цифровая подпись и инфраструктура открытых ключей (PKI): принципы работы, составные части PKI (удостоверяющий центр, регистрационный центр).
22. Протокол SSL/TLS: назначение, этапы рукопожатия (handshake), значение сертификатов для аутентификации сервера.
23. Принципы работы сетевых сканеров (Nmap) и анализаторов трафика (Wireshark) с точки зрения безопасности.
24. Классификация межсетевых экранов (брандмауэров): эволюция от packet filter до UTM и NGFW.
25. Принципы обнаружения и предотвращения вторжений (IDS/IPS): сравнение сигнатурного и аномального анализа.
26. Модель киберубийства (Cyber Kill Chain) Lockheed Martin: этапы целенаправленной атаки и точки противодействия.
27. Социальная инженерия: основные техники (фишинг, претекстинг, вишинг), цели и методы защиты.
28. Принцип безопасных настроек по умолчанию (Secure by Default) для ПО и СУБД.
29. Жизненный цикл разработки защищённого ПО (Secure SDLC): основные этапы и внедрение практик безопасности на каждом из них.
30. Статический анализ безопасности приложений (SAST): методология, типы обнаруживаемых дефектов, преимущества и ограничения.
31. Динамический анализ безопасности приложений (DAST): методология «серого ящика», примеры инструментов.
32. OWASP Top 10 2021: подробный разбор уязвимостей «Небезопасная десериализация» и «Недостатки журналирования и мониторинга».
33. Аутентификация: многофакторная аутентификация (MFA), биометрия, основанные на рисках системы.
34. Управление сессиями: безопасные методы генерации, хранения и инвалидации идентификаторов сессий.
35. Контроль доступа на уровне функций и данных в веб-приложениях.
36. Безопасная обработка ошибок и исключений: почему сообщения об ошибках не должны раскрывать внутреннюю структуру системы.
37. Безопасная загрузка файлов: основные риски (подмена, XSS, RCE) и методы защиты.
38. Реляционная модель данных с точки зрения безопасности: как структура таблиц и связей влияет на политики доступа.

39. Встроенные механизмы безопасности в СУБД (на примере PostgreSQL/MySQL): объекты безопасности (роли, профили, политики).
40. Инъекции NoSQL: принцип работы, отличия от SQLi, методы предотвращения.
41. Шифрование «на лету» (Transparent Data Encryption – TDE): архитектура, защищаемые данные, влияние на производительность.
42. Маскирование данных.
43. Журналирование (аудит) в СУБД.
44. Модель общей ответственности в облаках: разграничение обязанностей по безопасности между провайдером и клиентом.
45. Концепция «Непрерывная безопасность» (DevSecOps): интеграция практик и инструментов безопасности в процесс непрерывной интеграции и поставки (CI/CD), автоматизация проверок безопасности.
46. Управление секретами (Secrets Management) в разработке: безопасное хранение и использование паролей, ключей API, токенов доступа в средах разработки, тестирования и производства (на примере HashiCorp Vault, AWS Secrets Manager).
47. Контейнеризация и безопасность.
48. Управление идентификацией и доступом (IAM) в распределенных системах и микросервисных архитектурах: вызовы централизованной аутентификации, использование токенов (JWT), сервис-аккаунтов.
49. Юридические и этические аспекты тестирования на проникновение: понятие «разрешенного взлома», правила взаимодействия, оформление договоров и отчетности.
50. Обеспечение безопасности API (Application Programming Interface).

Темы для самостоятельной работы обучающихся

1. Сравнительный анализ моделей информационной безопасности: триада CIA, модель Паркера (шесть элементов), модель DIE.
2. Методологии моделирования угроз (Threat Modeling): STRIDE, PASTA, OCTAVE. Сравнение областей применения.
3. Принципы и этапы процесса управления рисками информационной безопасности: идентификация, оценка, обработка, мониторинг.
4. Классификация и анализ современных социально-инженерных атак: целевой фишинг (spear phishing), бизнес-компрометация email (BEC), принципы защиты.
5. Теоретические основы атак типа «отказ в обслуживании» (DoS/DDoS): классификация по уровням OSI, механизмы усиления (amplification), стратегии смягчения.
6. Понятие «Атакующая поверхность» (Attack Surface): методы анализа и сокращения для веб-приложения.
7. Эволюция и сравнительный анализ алгоритмов симметричного шифрования: от DES к AES и современным режимам работы (GCM, XTS).
8. Криптографические протоколы для безопасного удаленного доступа: сравнительный анализ SSH и TLS с точки зрения архитектуры и применения.
9. Теоретические основы криптографии на эллиптических кривых (ECC): преимущества перед RSA, области применения.

10. Принципы работы и архитектура инфраструктуры открытых ключей (PKI): роль корневых и промежуточных центров сертификации, жизненный цикл сертификата.
11. Квантовые вычисления и их потенциальное влияние на современную криптографию (криптоапокалипсис). Постквантовая криптография: основные направления.
12. Принципы архитектуры Zero Trust (Нулевого доверия): основные постулаты, отличия от периметровой модели, ключевые компоненты.
13. Модели зрелости безопасной разработки (BSIMM, OpenSAMM): сравнительный анализ и принципы использования для оценки процессов.
14. Теоретические основы статического (SAST) и динамического (DAST) анализа безопасности кода: внутренние механизмы, виды обнаруживаемых паттернов уязвимостей.
15. Формальные методы верификации программного обеспечения: теория и применение для обеспечения безопасности критических систем.
16. Уязвимости цепочки поставок программного обеспечения (Software Supply Chain): типы атак (компрометация зависимостей, злонамеренные коммиты), принципы защиты (SBOM).
17. Мандатные модели контроля доступа: детальный разбор моделей Белла-ЛаПадулы (конфиденциальность) и Бибы (целостность), их применение в СУБД.
18. Теоретические основы гомоморфного шифрования: принципы работы, потенциальные применения для защиты данных в облаке и БД.
19. Концепции и методы обеспечения конфиденциальности данных: анонимизация, псевдонимизация, дифференциальная приватность (differential privacy).
20. Архитектура и принципы работы систем управления секретами (Secrets Management) в DevOps-средах.
21. Внутренние механизмы транзакций в СУБД (ACID) с точки зрения обеспечения целостности данных и их взаимосвязь с журналами транзакций (WAL).
22. Архитектура и принципы работы систем обнаружения и предотвращения вторжений (IDS/IPS) на основе сигнатур и аномального поведения.
23. Теоретические основы сегментации сети (Network Segmentation) и микросегментации: цели, методы реализации, влияние на безопасность.
24. Стандарты и протоколы безопасной маршрутизации: анализ уязвимостей протоколов (например, BGP) и методов их защиты (RPKI).
25. Фазы жизненного цикла обработки инцидента информационной безопасности (NIST SP 800-61): подготовка, обнаружение, анализ, сдерживание, ликвидация, восстановление, извлечение уроков.
26. Сравнительный анализ международных стандартов информационной безопасности: ISO/IEC 27001, NIST Cybersecurity Framework, CIS Controls.
27. Регуляторные требования к защите персональных данных: сравнительный анализ GDPR (ЕС) и 152-ФЗ (РФ).
28. Этические кодексы и принципы в сфере информационной безопасности и хакерской этики.
29. Теоретические основы безопасности интернета вещей (IoT): специфические угрозы, архитектурные уязвимости, подходы к защите.
30. Современные тренды и будущее ИБ: влияние искусственного интеллекта (AI) и машинного обучения (ML) на кибербезопасность (как для защиты, так и для атак).

Примерные варианты тестовых оценочных заданий (ТОЗ) для контрольного рубежа в рамках текущего контроля

Тестовое задание	Оцениваемые компетенции
ВОПРОСЫ ОТКРЫТОГО ТИПА	
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Совокупность правовых, организационных и технических мер, направленных на защиту информации от угроз, называется информационной _____. +: безопасностью	ПК 1.5.
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Ключевой принцип обработки персональных данных, означающий, что оператор должен собирать только те данные, которые необходимы для заявленной цели, называется _____. +: ограничение обработки персональных данных	ОК 09.
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Свойство информации, означающее, что она не должна быть изменена или уничтожена несанкционированно, — это _____. +: целостность	ОК 01.
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Свойство безопасности, гарантирующее, что система или ресурсы доступны для использования авторизованными пользователями в любой момент времени, — это _____. +: доступность	ПК 1.4.
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Криптографический алгоритм, использующий один и тот же ключ для шифрования и дешифрования, называется _____ шифрованием +: симметричным	ПК 1.5.
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Стандарт шифрования, принятый в 2001 году как преемник DES, называется _____ +: Advanced Encryption Standard	ОК 02.
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Модель управления доступом, где права назначаются не пользователям напрямую, а ролям, которые они занимают, называется _____. +: ролевым доступом	ПК 1.4.
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Принцип информационной безопасности, согласно которому пользователь должен обладать минимальным набором привилегий, необходимым для выполнения своей работы, называется принципом _____. +: минимальных привилегий	ПК 1.5.

(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Одна из самых распространенных и опасных уязвимостей вебприложений, позволяющая внедрить произвольный SQL-код в запрос к базе данных, называется _____. +: SQL-инъекция	ПК 1.1.
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Тип вредоносного программного обеспечения, которое блокирует доступ к данным или системе и требует выкуп за его восстановление, называется _____. +: программой-вымогателем	ОК 01.
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Атака, целью которой является полное исчерпание ресурсов системы (канала связи, процессора, памяти) и приведение к отказу в обслуживании, называется _____ +: отказ в обслуживании	ОК 01.
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Язык SQL, используемый для назначения и отзыва прав доступа пользователей и ролей к объектам базы данных, называется языком управления _____ +: доступом	ПК 1.4.
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Процесс регулярного копирования данных для возможности их восстановления в случае утери или повреждения называется _____. +: резервное копирование	ПК 1.4.
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ)	ПК 1.5.

Технология шифрования, при которой данные на диске (табличном пространстве, файлах данных) шифруются и дешифруются автоматически, прозрачно для приложения, называется _____ шифрованием +: прозрачным	
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Запись действий пользователей и системы в специальный журнал для последующего анализа и расследования инцидентов в СУБД называется _____ +: аудит	ПК 1.5.
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Протокол, обеспечивающий защищенную передачу данных по сетям TCP/IP, на основе которого работает HTTPS, — это _____. +: TLS	ОК 09.

(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Программный или аппаратный барьер, контролирующий сетевой трафик между сегментами сети на основе заданных правил, называется _____. +: межсетевой экран	ОК 02.
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Международный стандарт, описывающий требования к системе менеджмента информационной безопасности, — это _____. +: ГОСТ Р ИСО/МЭК 27001	ОК 09.
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Процесс подтверждения подлинности пользователя или системы (например, с помощью логина и пароля) называется _____. +: аутентификация	ОК 01.
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Общепризнанная база данных для публикации информации об уязвимостях программного обеспечения использует идентификаторы формата _____. +: CVE	ОК 02.
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Процесс проверки исходного кода программы на наличие уязвимостей без его выполнения называется _____ анализом +: статическим	ПК 1.1.
ВОПРОСЫ ЗАКРЫТОГО ТИПА	
Какой федеральный закон Российской Федерации является основным, регулирующим обработку персональных данных операторами? -: 149-ФЗ «Об информации, информационных технологиях и о защите информации» +: 152-ФЗ «О персональных данных» -: 187-ФЗ «О безопасности критической информационной инфраструктуры» -: 98-ФЗ «О коммерческой тайне»	ОК 09.
Какой класс вредоносного программного обеспечения характеризуется способностью к саморепликации и распространению по сети без участия пользователя, эксплуатируя уязвимости в программном обеспечении?	ОК 01.

-: Вирус -: Троянская программа +: Сетевой червь -: Руткит	

Какая модель управления доступом предполагает, что права доступа к объекту назначаются его владельцем? -: Ролевая (RBAC) +: Дискреционная (DAC) -: Мандатная (MAC) -: Атрибутная (ABAC)	ПК 1.4.
Какой стандарт (алгоритм) является текущим мировым стандартом симметричного шифрования, рекомендованным для защиты конфиденциальной информации? -: DES (Data Encryption Standard) -: 3DES (Triple DES) -: RC4 (Rivest Cipher 4) +: AES (Advanced Encryption Standard)	ОК 02.
Что из перечисленного является ПРАВИЛЬНОЙ последовательностью этапов классического процесса управления рисками информационной безопасности? -: Обработка -> Идентификация -> Оценка -> Мониторинг +: Идентификация -> Оценка -> Обработка -> Мониторинг -: Оценка -> Мониторинг -> Идентификация -> Обработка -: Мониторинг -> Обработка -> Оценка -> Идентификация	ОК 01.
Основной целью какой фазы атаки по модели Cyber Kill Chain является закрепление злоумышленника в системе для длительного присутствия и достижения конечных целей? -: Разведка (Reconnaissance) -: Установка бэкдора (Installation) +: Закрепление (Establishment of Foothold) -: Выполнение целей (Actions on Objectives)	ОК 01.
Какой из перечисленных методов является НАИБОЛЕЕ эффективным для предотвращения атак типа SQL-инъекция на уровне прикладного кода? -: Валидация ввода на стороне клиента (в браузере) -: Экранирование специальных символов (например, кавычек) +: Использование параметризованных запросов (Prepared Statements) -: Частая смена паролей учетных записей БД	ПК 1.5.
Что из перечисленного является основной задачей системы DLP (Data Loss Prevention)? (ОК 01) -: Защита от сетевых атак типа DoS +: Предотвращение утечки конфиденциальной информации за пределы организации -: Шифрование данных на жестких дисках -: Обнаружение сетевых вторжений	ОК 01.

В рамках модели общей ответственности (Shared Responsibility Model) при использовании облачной услуги PaaS (Platform as a Service) за безопасность какой из перечисленных компонентов ОТВЕЧАЕТ КЛИЕНТ, а не провайдер? -: Физическая безопасность дата-центра -: Безопасность операционной системы и патчи для неё -: Безопасность сетевой инфраструктуры (маршрутизаторы, фаерволы)	ПК 1.5.
+: Безопасность прикладного кода и настройка прав доступа пользователей в приложении	

Шкала оценивания тестовых заданий

Данный вид контроля, рассчитан на выявление уровня усвоения теоретического и практического материала в рамках изучения дисциплин. Критерии оценивания теста: 1 вопрос = 1 балл.

Оценка «5»	30-27 Баллов
Оценка «4»	26-23 Баллов
Оценка «3»	22-18 Баллов
Оценка «2»	0-17 Баллов