Приложение к рабочей программе дисциплины

Федеральное государственное автономное образовательное учреждение высшего образования «Российский университет дружбы народов имени Патриса Лумумбы»

Факультет искусственного интеллекта

(наименование основного учебного подразделения (ОУП) – разработчика программы)

Кафедра информационной безопасности

(наименование базового учебного подразделения (БУП) – разработчика программы)

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ И БАЛЛЬНО-РЕЙТИНГОВАЯ СИСТЕМА ПО ДИСЦИПЛИНЕ

Методы и системы защиты информации, информационная безопасность

(наименование дисциплины/практики)

Научная специальность:

2.3.6. Методы и системы защиты информации, информационная безопасность

(шифр и наименование научной специальности)

Освоение дисциплины ведется в рамках реализации программы аспирантуры:

Методы и системы защиты информации, информационная безопасность

(наименование программы подготовки научных и научно-педагогических кадров)

2026 г.

1. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И САМОСТОЯТЕЛЬНОЙ РАБОТЫ АСПИРАНТОВ ПО ДИСЦИПЛИНЕ

ТЕСТИРОВАНИЕ используется для оценки качества освоения обучающимися части учебного материала дисциплины.

Верный ответ на каждый вопрос теста оценивается в 1 балл, итоговый балл за тест рассчитывается как сумма всех набранных баллов. В течение семестра тестирование проводится два раза по окончания освоения разделов 2 и 4 тематического плана дисциплины. В каждый тест входит 15 вопросов. Каждое тестирование оценивается от 0 до 15 баллов.

1. Что является основной целью обеспечения конфиденциальности информации?

а) Обеспечение постоянного доступа к информации.

б) Предотвращение несанкционированного раскрытия информации.

в) Защита от несанкционированного изменения информации.

г) Гарантия подлинности источника информации.

2. Какая математическая модель безопасности наиболее тесно связана с концепцией «невлияния» (non-interference)?

а) Модель Белла-ЛаПадулы.

б) Модель Кларка-Уилсона.

в) Модель Бибба.

г) Модель Гогена-Мезигера.

3. Какой современный подход к обеспечению ИБ предполагает создание «глубинной обороны» (Defense in Depth)?

а) Risk-based security.

б) Compliance-based security.

в) Многоуровневая защита.

г) Security by Obscurity.

4. Какой международный стандарт является основой для построения систем менеджмента информационной безопасности (СМИБ)?

а) ISO 27001.

б) ISO 9001.

в) RFC 2196.

г) NIST SP 800-53.

5. Какой из подходов к криптографическому изменению информации обеспечивает конфиденциальность данных при их обработке?

а) Использование протокола Диффи-Хеллмана.

б) Использование гомоморфного шифрования.

в) Использование протоколов SSL/TLS.

г) Использование электронной подписи (ЭП).

6. Основное отличие стеганографии от криптографии заключается в том, что стеганография:

а) Обеспечивает более высокую криптостойкость.

б) Использует более сложные математические алгоритмы.

в) Скрывает сам факт существования сообщения.

г) Требует обязательного использования секретного ключа.

7. Что из перечисленного НЕ является фактором многофакторной аутентификации?

а) Пин-код (что-то, что вы знаете).

б) Отпечаток пальца (что-то, что вы есть).

в) Мобильный телефон (что-то, что у вас есть).

г) Логин пользователя (что-то, что вы знаете).

8. Система, которая анализирует сетевой трафик и поведение системы для выявления подозрительной активности, известна как:

а) Межсетевой экран (Firewall).

б) Система обнаружения вторжений (IDS).

в) Система предотвращения утечек данных (DLP).

г) Антивирусное программное обеспечение.

9. Какой принцип архитектуры безопасности предполагает минимализацию привилегий пользователей и процессов?

а) Принцип разделения полномочий.

б) Принцип наименьших привилегий.

в) Принцип разделения обязанностей.

г) Принцип эшелонированной обороны.

10. Ключевой проблемой безопасности в модели облачных вычислений «ПО как услуга» (SaaS) является:

а) Физическая безопасность центра обработки данных.

б) Безопасность операционных систем гипервизоров.

в) Защита данных приложения от несанкционированного доступа.

г) Безопасность сетевой инфраструктуры провайдера.

11. Какой основной риск безопасности связан с технологией Big Data?

а) Низкая скорость обработки данных.

б) Сложность обеспечения конфиденциальности и целостности больших объемов разнородных данных.

в) Невозможность использования традиционных СУБД.

г) Отсутствие методов анализа данных.

12. Что представляет собой основную угрозу для мобильных систем?

а) Физическая поломка устройства.

б) Установка приложений из неофициальных источников (sideloading).

в) Ограниченная емкость батареи.

г) Низкая производительность процессора.

13. Какой документ является основополагающим для стратегического управления ИБ в организации?

а) Политика информационной безопасности.

б) Инструкция по резервному копированию.

в) Отчет об инциденте.

г) Журнал учета посетителей.

14. Какой этап управления инцидентами безопасности является первым?

а) Устранение последствий инцидента.

б) Анализ причины инцидента.

в) Обнаружение и регистрация инцидента.

г) Пост-инцидентный анализ.

15. Какой показатель НЕ используется для оценки эффективности систем защиты информации?

а) KPI (Ключевые показатели эффективности).

б) KRI (Ключевые показатели риска).

в) ROI (Возврат на инвестиции).

г) CPU Utilization (Загрузка центрального процессора).

16. Модель непрерывного совершенствования процессов обеспечения ИБ, такая как PDCA (Plan-Do-Check-Act), наиболее тесно связана с:

а) Моделью зрелости процессов CMMI.

б) Моделью Белла-ЛаПадулы.

в) Криптографическим протоколом Диффи-Хеллмана.

г) Технологией блокчейн.

17. Основная угроза, которую несут квантовые компьютеры для современной криптографии, – это:

а) Взлом алгоритмов симметричного шифрования (например, AES-256).

б) Взлом хэш-функций (например, SHA-256).

в) Взлом асимметричных алгоритмов на основе факторизации и дискретного логарифмирования (например, RSA, ECC).

г) Полное обесценивание стеганографических методов.

18. Как технологии искусственного интеллекта применяются в системах защиты информации?

а) Для замены системных администраторов.

б) Для автоматического написания безопасного кода.

в) Для поведенческого анализа и выявления аномалий в реальном времени.

г) Для физической охраны помещений.

19. Что является основным преимуществом биометрических систем нового поколения, использующих несколько биометрических параметров (мультимодальных)?

а) Более низкая стоимость.

б) Повышенная скорость аутентификации.

в) Более высокая надежность и устойчивость к спуфингу.

г) Полная анонимность пользователя.

20. Какое свойство технологии «блокчейн» является ключевым для обеспечения целостности и неизменяемости данных?

а) Децентрализация и распределенный реестр.

б) Наличие в каждом блоке хэш-суммы предыдущего блока.

в) Анонимность всех участников.

г) Использование только симметричного шифрования.

21. Если злоумышленник подменил данные в журнале регистрации (log-файле), какое свойство информации было нарушено?

а) Конфиденциальность.

б) Целостность.

в) Доступность.

г) Аутентичность.

22. Какой из перечисленных стандартов является де-факто международным ориентиром (benchmark) для построения системы менеджмента информационной безопасности и служит основой для многих национальных стандартов?

а) COBIT.

б) ISO/IEC 27001.

в) NIST SP 800-53.

г) ITIL.

23. Какая комбинация методов защиты является наиболее эффективной против целевых атак (APT)?

а) Антивирус + Межсетевой экран.

б) Система обнаружения вторжений + Стеганографический инструмент.

в) Многофакторная аутентификация + Система предотвращения утечек данных (DLP) + Анализ поведенческих аномалий.

г) Политика строгих паролей + Регулярное обновление ОС.

24. При переходе компании на облачную инфраструктуру (IaaS) ответственность за безопасность какой компоненты лежит на компании (клиенте поставщика облачных услуг)?

а) Физическая безопасность дата-центра.

б) Безопасность гипервизора.

в) Безопасность операционной системы развернутых виртуальных машин.

г) Безопасность каналов связи между дата-центрами.

25. Какая из перечисленных метрик наиболее полезна для высшего руководства при оценке стратегической эффективности управления ИБ?

а) Количество заблокированных межсетевым экраном пакетов в час.

б) Процент сотрудников, прошедших обучение по ИБ.

в) Среднее время на устранение инцидента безопасности (MTTR).

г) Количество успешно отраженных DDoS-атак.

26. Какая технология из «перспективных направлений» может кардинально решить проблему доверия в распределенных системах без необходимости в центральном арбитре?

а) Квантовая криптография.

б) Искусственный интеллект.

в) Биометрия.

г) Блокчейн.

27. Сценарий: в организации произошла утечка данных. Расследование показало, что сотрудник, имевший доступ к информации, передал ее третьим лицам. Нарушение какого принципа модели Кларка-Уилсона стало причиной инцидента?

а) Принцип простоты.

б) Принцип разделения обязанностей.

в) Принцип неотказуемости.

г) Принцип сертифицированных и разрешенных трансформаций.

28. Какой инструмент управления рисками ИБ напрямую связан с принципами управления информационной безопасностью?

а) Построение матрицы вероятности и воздействия рисков.

б) Настройка криптографического протокола TLS 1.3.

в) Внедрение системы стеганографии для скрытой передачи данных.

г) Разработка алгоритма машинного обучения для обнаружения аномалий.

29. Какое из следующих утверждений лучше всего описывает концепцию «Security by Design»?

а) Безопасность рассматривается как дополнение к готовому продукту.

б) Вопросы безопасности интегрируются в процесс разработки системы на самых ранних этапах.

в) Безопасность обеспечивается исключительно за счет строгих политик доступа.

г) Безопасность системы проверяется только на этапе тестирования.

30. Сценарий: для защиты критической инфраструктуры предлагается использовать систему, которая сочетает поведенческий анализ для выявления аномалий в реальном времени и технологию распределенного реестра для гарантии целостности и неизменности журналов событий. Какие два перспективных направления, применяемых в сфере ИБ, объединяются в этом решении?

а) Квантовые технологии и биометрические системы.

б) Биометрические системы и искусственный интеллект.

в) Технологии искусственного интеллекта и блокчейн.

г) Блокчейн и квантовые технологии.

Ключи к тесту

1. б	2. г	3. в	4. а	5. б	6. в	7. г	8. б	9. б	10. в
11. б	12. б	13. а	14. в	15. г	16. а	17. в	18. в	19. в	20. б
21. б	22. б	23. в	24. в	25. в	26. г	27. г	28. а	29. б	30. в

КОНТРОЛЬНАЯ РАБОТА используется для оценки качества освоения обучающимися части учебного материала дисциплины.

Контрольная работа проводится три раза в течение семестра по окончании освоения аспирантов разделов 1, 3 и 5 тематического плана дисциплины. В каждую контрольную работу

входит два вопроса – теоретический и практико-ориентированный. Контрольная работа выполняется в письменном виде. За каждую контрольную работу можно получить от 0 до 10 баллов.

Примерный перечень вопросов и заданий, выносимых на контрольную работу:

Теоретические вопросы:

1. Раскройте суть модели Кларка-Уилсона. Опишите её ключевые компоненты (CDI, UDI, TP, IVP) и основные принципы обеспечения целостности данных. В чём её фундаментальное отличие от модели Белла-ЛаПадулы?

2. Дайте сравнительную характеристику криптографических протоколов SSL/TLS и IPsec. Опишите их архитектурные особенности, основные этапы установления защищённого соединения и типичные сценарии применения.

3. Опишите архитектуру безопасности модели «Платформа как услуга» (PaaS). Распределите зоны ответственности за безопасность между облачным провайдером и клиентом. Перечислите ключевые риски и контрмеры, находящиеся в зоне ответственности клиента.

4. Опишите жизненный цикл управления инцидентами информационной безопасности (от подготовки до пост-инцидентного анализа). Каковы цели и основные результаты каждого этапа?

5. Проанализируйте угрозы и возможности, которые несут квантовые вычисления для сферы информационной безопасности. Дайте характеристику алгоритмам «квантового взлома» (Шора, Гровера) и опишите принципы работы методов «постквантовой криптографии» и «квантового распределения ключей» (QKD).

Практико-ориентированные вопросы:

1. Вам поручено провести качественную оценку защищённости системы дистанционного банковского обслуживания (ДБО) для физических лиц. Разработайте упрощённую модель угроз, выделив не менее 4 ключевых активов, не менее 3 актуальных угроз для каждого актива и уязвимости, которые эти угрозы могут эксплуатировать.

2. Разработайте схему применения методов стеганографии для скрытой маркировки конфиденциальных документов, передаваемых в виде файлов в формате PDF. Опишите, какие метки могут быть внедрены, в какие элементы документа, и как будет осуществляться проверка подлинности и факта утечки в случае инцидента.

3. На предприятии планируется внедрение системы Big Data для анализа поведения пользователей. Сформулируйте не менее 5 конкретных требований к защите данных в рамках этого проекта, учитывая жизненный цикл данных (сбор, хранение, обработка, передача, уничтожение) и положения законодательства о персональных данных.

4. Практико-ориентированный вопрос: По итогам года в организации было зарегистрировано 15 инцидентов ИБ. Проанализируйте следующие данные и предложите 3-4 стратегических решения для руководства, направленных на снижение количества подобных инцидентов в будущем:

10 инцидентов – фишинг и утечка учётных данных.

3 инцидента – установка сотрудниками нелицензионного ПО.

2 инцидента – потеря мобильных устройств с корпоративной почтой.

5. Предложите концепцию системы контроля доступа в secure area (помещение с серверным оборудованием) на основе мультимодальной биометрии. Опишите, какие два биометрических фактора будут использоваться и почему, как будет организован процесс верификации/идентификации, и какие меры будут приняты для защиты биометрических шаблонов от компрометации.

Таблица 1. Шкала и критерии оценки контрольной работы

Критерии оценки контрольной работы	Баллы		
	Не соответствует критерию	**Частично соответствует критерию**	**Полностью соответствует критерию**
Правильность и полнота выполнения заданий	0	1-4	5
Правильность выводов по полученным результатам	0	1-4	5
ИТОГО			**10**

2. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

Промежуточная аттестация по дисциплине «Методы и системы защиты информации, информационная безопасность» проводится в форме аттестационного испытания **по итогам изучения дисциплины**. Вид аттестационного испытания – **кандидатский экзамен**.

Аттестационное испытание проводится по билетам, содержащим три вопроса по курсу дисциплины.

Вопросы для подготовки к аттестационному испытанию по дисциплине «Методы и системы защиты информации, информационная безопасность»:

1. Эволюция понятия «информационная безопасность»: от классической триады CIA к современным расширенным моделям.
2. Методологический принцип «нулевого доверия» (Zero Trust) и его влияние на архитектуру информационных систем.
3. Сравнительный анализ детерминистических и вероятностных моделей безопасности информационных систем.
4. Философско-методологические аспекты обеспечения ИБ: соотношение категорий «угроза», «уязвимость», «риск» и «защита».
5. Системные ограничения и границы применимости формальных моделей безопасности Белла-ЛаПадулы, Биба и Кларка-Уилсона.
6. Место и роль человеческого фактора в современных методологиях обеспечения информационной безопасности.
7. Проблема обеспечения безопасности цепочек поставок программного обеспечения (Software Supply Chain Security) как ключевой вызов для современных методологий защиты информации.
8. Подходы к управлению рисками информационной безопасности.
9. Возможности и ограничения теории игр при моделировании взаимодействия атакующего и защитника.
10. Современные тенденции развития национальных и международных стандартов информационной безопасности (ISO/IEC 27000, NIST CSF).
11. Математические основы и практическая значимость концепции «невлияния» (non-interference) для обеспечения конфиденциальности.
12. Проблемы количественной оценки рисков ИБ: достоинства и недостатки различных методов.
13. Критерии выбора и адаптации международных стандартов ИБ для построения СМИБ в организации.
14. Роль сертификации в контексте обеспечения доверия на национальном и транснациональном уровнях.
15. Сравнительный анализ задач и методов криптографии и стеганографии.
16. Архитектурные принципы и области применения криптографических протоколов нового поколения.

17. Проблема управления ключевой информацией в больших распределенных системах и современные подходы к созданию PKI.

18. Системные уязвимости и ограничения существующих технологий многофакторной аутентификации.

19. Фундаментальные отличия систем обнаружения вторжений (IDS) от систем предотвращения вторжений (IPS).

20. Проблема обеспечения безопасности на протяжении всего жизненного цикла разработки ПО (Secure SDLC).

21. Принципы проектирования безопасной архитектуры микросервисов.

22. Модель ответственности за безопасность в сервисных моделях облачных вычислений (IaaS, PaaS, SaaS).

23. Специфические угрозы безопасности больших данных (Big Data) на различных этапах их жизненного цикла.

24. Концепции «безопасность как код» (Security as Code) и «инфраструктура как код» (IaC) в контексте управления рисками.

25. Особенности обеспечения безопасности в сетях мобильной связи 5G и последующих поколений.

26. Проблема безопасности «Интернета вещей» (IoT) как проявление системного кризиса.

27. Содержание и взаимосвязь стратегического, тактического и операционного уровней управления ИБ.

28. Методологии оценки экономической эффективности инвестиций в информационную безопасность (ROI, ROSI).

29. Модель зрелости процессов управления ИБ и её соотношение с циклом Деминга-Шухарта (PDCA).

30. Цели, задачи и организационные модели центров мониторинга и управления инцидентами безопасности (SOC, CERT/CSIRT).

31. Реактивная и проактивная парадигмы управления рисками ИБ.

32. Необходимость интеграции системы управления ИБ (СМИБ) с системами общего менеджмента организации.

33. Влияние квантовых вычислений на современную криптографию и перспективы постквантовой криптографии.

34. Потенциал и фундаментальные ограничения технологий искусственного интеллекта в задачах обнаружения кибератак.

35. Этические и правовые вызовы, связанные с применением систем биометрической идентификации нового поколения.

36. Роль технологии блокчейн и распределенного реестра (DLT) в построении систем обеспечения доверия.

37. Научно-исследовательские задачи в области защиты критической информационной инфраструктуры (КИИ) от целевых атак (APT).

38. Влияние концепций «цифровых двойников» и «метавселенных» на ландшафт угроз ИБ.

39. Проблема «исчезновения периметра» (de-perimeterization) и её влияние на эволюцию концепций защиты.

40. Кибербезопасность как элемент гибридных войн и инструмент геополитического противостояния.

41. Содержание и правовая оценка проблемы атрибуции кибератак.

42. Взаимосвязь и противоречия между обеспечением информационной безопасности и защитой персональных данных.

43. Современные тенденции в развитии нормативно-правового регулирования в области ИБ на международной арене.

44. Проблема безопасности цепочек поставок (Supply Chain Security) в контексте ИБ.

45. Особенности обеспечения безопасности систем промышленного IoT (IIoT) и АСУ ТП.

46. Содержание и примеры использования методов формальной верификации для доказательства безопасности компонентов.

47. Феномен «устаревания безопасности» (security decay) и его причины.

48. Психологические и социотехнические аспекты формирования культуры информационной безопасности в организации.

49. Проблема «информационной перегрузки» оператора SOC и современные подходы к её решению.

50. Основные глобальные вызовы и перспективные направления фундаментальных научных исследований в области ИБ.

Таблица 2. Шкала и критерии оценивания ответов обучающихся на аттестационном испытании

Критерии оценки ответа	**Баллы**		
	Ответ не соответствует критерию	**Ответ частично соответствует критерию**	**Ответ полностью соответствует критерию**
Обучающийся дает ответ без наводящих вопросов преподавателя	0	1-7	8
Обучающийся практически не пользуется подготовленной рукописью ответа	0	1-7	8
Ответ показывает уверенное владение обучающего терминологическим и методологическим аппаратом дисциплины/модуля	0	1-7	8
Ответ имеет четкую логическую структуру	0	1-7	8
Ответ показывает понимание обучающимся связей между предметом вопроса и другими разделами дисциплины/модуля и/или другими дисциплинами/ модулями ОП	0	1-7	8
ИТОГО, баллов за ответ			**40**

3. БАЛЛЬНО-РЕЙТИНГОВАЯ СИСТЕМА

Контролируемый раздел дисциплины	Контролируемая тема дисциплины	ФОСы (формы контроля уровня освоения ОПП)								Баллы темы	Баллы раздела
		Аудиторная работа					СР				
		Опрос	Тест	Коллоквиум	Контрольная работа	Кейс-задача	Выполнение ДЗ	Реферат	Канд. экзамен		
1	2	3	4	5	6	7	8	9	10	11	12
Раздел 1. Теория информационной безопасности	Тема 1. Теоретические основы и методология обеспечения информационной безопасности Тема 2. Математические модели и методы оценки защищенности информационных систем Тема 3. Современные концепции и подходы к обеспечению информационной безопасности Тема 4. Национальные и международные стандарты и системы сертификации в области информационной безопасности				10				8	18	18
Раздел 2. Современные методы защиты информации	Тема 1. Криптографические протоколы и системы защиты нового поколения Тема 2. Методы стеганографии и их применение в системах защиты Тема 3. Технологии многофакторной аутентификации и идентификации		15						8	23	23

	Тема 4. Системы обнаружения и предотвращения продвинутых угроз (APT)										
Раздел 3. Комплексные системы защиты информации	Тема 1. Архитектура современных систем защиты информационных инфраструктур Тема 2. Методы обеспечения безопасности облачных вычислений Тема 3. Защита больших данных и систем Big Data Тема 4. Безопасность мобильных и распределенных систем				10				8	18	18
Раздел 4. Управление информационной безопасностью	Тема 1. Стратегическое управление ИБ в организации Тема 2. Системы управления инцидентами безопасности Тема 3. Методологии оценки эффективности систем защиты информации Тема 4. Модель непрерывного совершенствования процессов обеспечения ИБ		15						8	23	23
Раздел 5. Перспективные направления развития сферы ИБ	Тема 1. Квантовые технологии в области защиты информации Тема 2. Искусственный интеллект и машинное обучение в системах защиты информации Тема 3. Биометрические системы нового поколения Тема 4. Технология «блокчейн» и ее применение в задачах обеспечения ИБ				10				8	18	18
Всего			**30**		**30**				**40**	**100**	**100**