Московский Институт Психоанализа

Негосударственное образовательное частное учреждение
высшего образования «Московский институт психоанализа»
(НОЧУ ВО «Московский институт психоанализа»)

# ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

## ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

| | |
|---|---|
| Направление подготовки/специальность | **44.03.05 Педагогическое образование (с двумя профилями подготовки)** |
| Направленность (профиль/специализация) | **Иностранный язык (английский) и информационные технологии в образовании** |
| Уровень высшего образования | **Бакалавриат** |
| Форма обучения | **Очная** |

Москва 2026

1. **Фонд оценочных средств для проведения текущего контроля успеваемости**

**Задания для проведения текущего контроля успеваемости** (темы докладов, рефератов, эссе, тестовые задания, кейсовые задания и т.п.) (а также, обязательно представить задания для подготовки к практическим занятиям, а также критерии и шкалу оценивания к ним)

**Вопросы для устного опроса.**

1. Раскройте содержание принципа целеполагания обработки персональных данных согласно ст. 5 ФЗ № 152-ФЗ. Каковы правовые последствия хранения избыточных биометрических данных обучающихся в школьной базе?
2. Охарактеризуйте модель угроз информационной безопасности образовательного учреждения. Классификация нарушителей (внутренний vs внешний) и их мотивация применительно к вузовской инфраструктуре.
3. Сформулируйте требования законодательства РФ к локализации баз данных российских граждан (*Data Localization*). Риски использования зарубежных облачных LMS (Google Classroom, Microsoft Teams) без переноса серверов в РФ.
4. Разграничьте понятия «коммерческая тайна», «служебная тайна» и «персональные данные». Правовой режим доступа преподавателя к зачетным книжкам и ведомостям других групп.
5. Организационные меры защиты информации. Политика чистого стола (*Clean Desk Policy*) и чистого экрана (*Clear Screen Policy*) как элементы системы менеджмента информационной безопасности (СМИБ).
6. Процедура классификации информационных систем персональных данных (ИСПДн). Определение уровня защищенности (УЗ-1 – УЗ-4) для базы данных студентов педагогического вуза.
7. Ответственность оператора персональных данных (ст. 13.11 КоАП РФ vs ст. 137 УК РФ). Алгоритм действий педагога при обнаружении утечки списка контактов родителей класса.
8. Концепция BYOD (*Bring Your Own Device*) в школе: анализ вектора атаки *Man-in-the-Middle* через незащищенные точки доступа Wi-Fi и методы контейнеризации корпоративных данных.
9. Инциденты информационной безопасности: инцидент, авария, сбой. Методология реагирования на инциденты (Incident Response Lifecycle) согласно рекомендациям НКЦКИ (ГосСОПКА).
10. Цифровая гигиена педагога. Управление цифровой репутацией (*Digital Footprint*) и этические аспекты ведения личных аккаунтов в социальных сетях при наличии учеников в друзьях.
11. Симметричное и асимметричное шифрование. Механизм работы протокола TLS при авторизации в электронной зачетной книжке и проблема управления ключами.
12. Электронная подпись (ЭП) в образовании. Различие между простой, усиленной неквалифицированной и усиленной квалифицированной ЭП при подписании приказов о зачислении.
13. Социальная инженерия: техника фишинга (*Spear Phishing*) против сотрудников деканата. Психологические триггеры и методы превентивного обучения персонала.
14. Технология DLP (*Data Loss Prevention*). Принципы фильтрации исходящего трафика для предотвращения несанкционированной выгрузки реестра абитуриентов из CRM-системы вуза.
15. Многофакторная аутентификация (MFA). Оценка эффективности методов второго фактора (SMS-код или OTP-токен или аппаратный ключ FIDO2) для доступа к административной части СДО.

16. Вредоносное ПО: разграничение понятий вируса, червя и трояна. Специфика атак программ-вымогателей (*Ransomware*) на файловые хранилища кафедр перед началом сессии.

17. Стеганография и криптография. Методы сокрытия факта передачи информации в метаданных изображений портфолио студентов.

18. Защита беспроводных сетей. Уязвимости протокола WPS и преимущества перехода на WPA3-Enterprise с использованием RADIUS-серверов в кампусе университета.

19. Резервное копирование (*Backup*) и восстановление после сбоев (*Disaster Recovery*). Стратегии Grandfather-Father-Son (GFS) для обеспечения непрерывности учебного процесса.

20. Аудит информационной безопасности. Логи сервера (*Syslog*) как доказательная база при расследовании инцидента несанкционированного изменения оценок в электронном журнале.

21. Информационная безопасность несовершеннолетних. Реализация контентной фильтрации в соответствии с ФЗ № 436-ФЗ («О защите детей от информации...») на уровне провайдера и школьного шлюза.

22. Кибербуллинг (*Cyberbullying*) в образовательной среде. Методика выявления признаков травли в школьных чатах и правовой алгоритм пресечения агрессии со стороны родителей.

23. Цифровое гражданство (*Digital Citizenship*). Формирование у обучающихся навыков критической оценки фейковых новостей (медиаграмотность) и проверки фактов (*Fact-checking*).

24. Безопасность дистанционного тестирования. Технологии прокторинга: алгоритмы анализа взгляда, распознавания лиц и шумового фона для предотвращения списывания.

25. Промышленный шпионаж в науке. Защита интеллектуальной собственности кафедры (черновики статей, диссертации до публикации) от кражи конкурентными организациями.

## Критерии и шкалы оценивания работы студентов на практических/лабораторных занятиях

| Оценка | Критерии оценивания |
|---|---|
| «отлично» | **Оценка «отлично»** выставляется, если студент активно работает в течение всего практического занятия, дает полные ответы на вопросы преподавателя в соответствии с планом практического занятия и показывает при этом глубокое овладение лекционным материалом, знание соответствующей литературы и законодательства, способен выразить собственное отношение по данной проблеме, проявляет умение самостоятельно и аргументированно излагать материал, анализировать явления и факты, делать самостоятельные обобщения и выводы, правильно выполняет учебные задачи. |
| «хорошо» | **Оценка «хорошо»** выставляется при условии: студент активно работает в течение практического занятия, вопросы освещены полно, изложения материала логическое, обоснованное фактами, со ссылками на соответствующие нормативные документы и литературные источники, освещение вопросов завершено выводами, студент обнаружил умение анализировать факты и события, а также выполнять учебные задания. Но в ответах допущены неточности, некоторые незначительные ошибки, имеет место недостаточная аргументированность при изложении материала, четко выраженное отношение студента к фактам и событиям. |
| «удовлетворительно» | **Оценка «удовлетворительно»** выставляется в том случае, когда студент в целом овладел сути вопросов по данной теме, обнаруживает знание лекционного материала, законодательства и учебной литературы, пытается анализировать факты и события, делать выводы и решать задачи. Но на занятии ведет себя |

| | |
|---|---|
| | пассивно, отвечает только по вызову преподавателя, дает неполные ответы на вопросы, допускает грубые ошибки при освещении теоретического материала. |
| «неудовлетворительно» | **Оценка «неудовлетворительно»** выставляется в случае, когда студент обнаружил несостоятельность осветить вопрос вопросы освещены неправильно, бессистемно, с грубыми ошибками, отсутствуют понимания основной сути вопросов, выводы, обобщения. |

## 2. Фонд оценочных средств для проведения промежуточной аттестации

**Задания для проведения промежуточной аттестации по итогам освоения дисциплины (тестовые задания, кейсовые задания и т.п.)**

1. **Согласно ФЗ № 152 «О персональных данных», трансграничная передача данных в страны, не обеспечивающие адекватную защиту, требует:**
   А) Только уведомления провайдера интернета.
   Б) Наличия письменного согласия субъекта или договора, стороной которого он является (за исключением узкого круга случаев).
   В) Публикации данных в газете.
   Г) Разрешения от министерства образования другой страны.
2. **Основной вектор атаки типа "Phishing" направлен на эксплуатацию:**
   А) Ошибок в коде ядра операционной системы.
   Б) Человеческого фактора (психологической доверчивости) для получения учетных данных легитимного пользователя.
   В) Перебора паролей (*Brute-force*) суперкомпьютером.
   Г) Отсутствия антивируса.
3. **В модели CIA (Confidentiality, Integrity, Availability) свойство "Integrity" (целостность) означает:**
   А) Доступность файла 24/7.
   Б) Свойство сохранения точности и полноты информации, гарантирующее отсутствие несанкционированных модификаций.
   В) Шифрование данных.
   Г) Удаление старых файлов.
4. **Усиленная квалифицированная электронная подпись (УКЭП) отличается от неквалифицированной тем, что:**
   А) Она написана синими чернилами.
   Б) Выдается только аккредитованным удостоверяющим центром и имеет юридическую силу собственноручной подписи согласно ФЗ № 63.
   В) Ее можно использовать только один раз.
   Г) Она бесплатна для всех граждан.
5. **Принцип минимальных привилегий (*Least Privilege Principle*) предписывает пользователю предоставлять:**
   А) Максимально возможные права администратора.
   Б) Только тот объем прав доступа, который строго необходим для выполнения его должностных обязанностей (например, преподаватель видит только своих студентов).
   В) Доступ ко всем базам данных вуза сразу.
   Г) Права случайным образом.
6. **Атака SQL Injection (инъекция кода) возможна в системе электронного журнала, если:**

А) Сервер находится в подвале.
Б) Входные данные пользователя (логин/пароль) конкатенируются с SQL-запросом без предварительной санитизации (экранирования спецсимволов).
В) Используется браузер Chrome.
Г) Монитор выключен.

7. **Хэширование паролей в базе данных необходимо для того, чтобы:**
А) Пароли было легче запомнить.
Б) Даже администратор СУБД не мог узнать исходный пароль пользователя, имея доступ к дампу таблицы (необратимое преобразование).
В) Увеличить скорость интернета.
Г) Сортировать пользователей по алфавиту.
8. **DLP-система (Data Loss Prevention) классифицирует документ как содержащий ПДн, если обнаруживает в нем:**
А) Слово "Привет".
Б) Паттерны, соответствующие формату паспортных данных, ИНН, СНИЛС или email-адресов, используя регулярные выражения.
В) Картинку здания школы.
Г) Дату вчерашнего дня.
9. **Основное отличие вредоносного ПО "Троян" от "Компьютерного червя":**
А) Цвет иконки программы.
Б) Троян — это маскирующееся полезное ПО, требующее действия пользователя; червь — самораспространяющийся код, использующий уязвимости сети.
В) Червь работает только ночью.
Г) Троян бесплатный.
10. **Двухфакторная аутентификация (2FA) считается нарушенной, если оба фактора относятся к одной категории (например):**
А) Пароль + SMS-код.
Б) Пароль + PIN-код (оба фактор "то, что вы знаете"), так как они могут быть скомпрометированы одновременно при подглядывании.
В) Пароль + Отпечаток пальца.
Г) Пароль + USB-токен.
11. **Стандарты серии ISO/IEC 27001 регламентируют:**
А) Скорость печати принтеров.
Б) Требования к системе менеджмента информационной безопасности (СМИБ) организации на основе риск-ориентированного подхода.
В) Качество бумаги в архиве.
Г) График отпусков ИТ-отдела.
12. **Обработка специальных категорий персональных данных (состояние здоровья, политические взгляды) в университете допускается:**
А) По желанию охранника.
Б) Только с письменного согласия субъекта или в случаях, прямо предусмотренных законодательством (например, медпункт общежития).
В) Если студент получил двойку.
Г) Для рассылки рекламы спортзала.
13. **Протокол HTTPS обеспечивает конфиденциальность передаваемых данных за счет:**
А) Использования очень длинных URL.

Б) Установления зашифрованного туннеля поверх TCP/IP с помощью протоколов SSL/TLS.
В) Запрета на использование картинок.
Г) Увеличения шрифта текста.

14. **Социальная атака "Pretexting" (создание предлога) заключается в:**
А) Отправке письма с вирусом.
Б) Создании фиктивного сценария (выдача себя за IT-поддержку, ректора, инспектора) для выуживания информации у жертвы.
В) Поломке клавиатуры.
Г) Обновлении Windows.
15. **Контрольная сумма (Hash Sum) файла используется для проверки:**
А) Красоты интерфейса.
Б) Целостности дистрибутива ПО (отсутствие повреждений при скачивании) путем сравнения хэша оригинала и полученного файла.
В) Автора картинки.
Г) Цены лицензии.
16. **Законодательное требование хранить персональные данные граждан РФ на серверах, расположенных на территории России, называется:**
А) Локализация данных.
Б) Глобализация данных.
В) Виртуализация данных.
Г) Архивация данных.
17. **Основная угроза публичного Wi-Fi в кафе рядом с университетом — это:**
А) Низкая скорость загрузки.
Б) Отсутствие шифрования канала, позволяющее злоумышленнику перехватывать трафик (Sniffing) и сессионные куки.
В) Высокая стоимость кофе.
Г) Наличие розеток.
18. **Биометрическая система идентификации по лицу может быть обманута (Presentation Attack) с помощью:**
А) Громкого звука.
Б) Фотографии высокого разрешения, видео на планшете или 3D-маски (спуфинг), если нет проверки Liveness Detection.
В) Яркого света.
Г) Закрытой двери.
19. **Политика управления паролями должна запрещать использование:**
А) Букв латинского алфавита.
Б) Паролей по умолчанию (default passwords), словарных слов и предсказуемых последовательностей (123456, Password).
В) Длины более 8 символов.
Г) Специальных знаков.
20. **Процедура удаления данных без возможности восстановления (Secure Deletion) выполняется методом:**
А) Перемещения в корзину.
Б) Затирки (Wiping/Purging) секторов диска нулями или случайными данными согласно стандарту DoD/NIST.
В) Переименования файла.
Г) Изменения расширения файла на .txt.

21. **Кибергигиена преподавателя включает обязательную проверку вложений на наличие макросов (*Macros Virus*) в файлах формата:**
    А) JPG.
    Б) DOC/DOCX и XLS/XLSX, которые могут содержать исполняемый код Visual Basic for Applications (VBA).
    В) PDF (текстовый слой).
    Г) MP3.
22. **Цифровой след (Digital Shadow) формируется из данных, размещенных о человеке:**
    А) Только им самим.
    Б) Третьими лицами (коллегами, студентами, системами видеонаблюдения) без прямого участия самого субъекта.
    В) В бумажном дневнике.
    Г) На заборе.
23. **При реализации концепции Zero Trust ("Никому не доверяй") периметральная защита межсетевым экраном (Firewall):**
    А) Считается достаточной мерой.
    Б) Дополняется микросегментацией и строгой проверкой каждого запроса внутри сети, независимо от его источника.
    В) Полностью отключается.
    Г) Заменяется на камеру наблюдения.
24. **Инцидент нарушения доступности (Availability Breach) в образовательном контексте чаще всего представлен как:**
    А) Опечатка в расписании.
    Б) DDoS-атака на сайт приемной комиссии в день подачи документов, делающая систему недоступной для легитимных пользователей.
    В) Смена логотипа вуза.
    Г) Приход нового ректора.
25. **Главная цель проведения киберучений (*Tabletop Exercise*) для администрации школы — это:**
    А) Проверка физической силы охраны.
    Б) Отработка регламентов взаимодействия (Communication Tree) и принятие решений в условиях симуляции инцидента ИБ до наступления реального кризиса.
    В) Продажа старого оборудования.
    Г) Выбор новой формы для учителей.

**Ключи к тестовым заданиям:** 1-Б, 2-Б, 3-Б, 4-Б, 5-Б, 6-Б, 7-Б, 8-Б, 9-Б, 10-Б, 11-Б, 12-Б, 13-Б, 14-Б, 15-Б, 16-А, 17-Б, 18-Б, 19-Б, 20-Б, 21-Б, 22-Б, 23-Б, 24-Б, 25-Б.

**Критерии и шкала оценивания:**

| Оценка | Количество баллов |
|---|---|
| «отлично» /зачтено | 83-100 баллов |
| «хорошо»/ зачтено | 68-82 балла |
| «удовлетворительно»/ зачтено | 50-67 баллов |
| «неудовлетворительно»/ не зачтено | 0-49 баллов |