Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Гриб Владислав Валерьевич
Должность: Ректор
Дата подписания: 23.11.2026 19:47:18
Уникальный программный ключ:
637517d24e103c3db032acf37e[illegible]

Образовательное частное учреждение высшего образования
«МОСКОВСКИЙ УНИВЕРСИТЕТ ИМЕНИ А.С. ГРИБОЕДОВА»
(ИМПЭ им. А.С. Грибоедова)

ИНСТИТУТ МЕЖДУНАРОДНОЙ ЭКОНОМИКИ, ЛИДЕРСТВА И МЕНЕДЖМЕНТА

УТВЕРЖДАЮ
Директор института
информационных технологий
и бизнес-информатики
_____ Т.В. Новикова
«14» сентября 2026г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Информационная безопасность и защита данных

Направление подготовки
09.04.03 Прикладная информатика
(уровень магистратура)

Направленность (профиль):
«Прикладная информатика в экономических и социальных системах»

Форма обучения: **очная**

Москва

Фонд оценочных средств дисциплины «Информационная безопасность и защита данных». Направление подготовки 09.04.03 Прикладная информатика, направленность (профиль): «Прикладная информатика в экономических и социальных системах» / О.А. Левичев – М.: ИМПЭ им. А.С. Грибоедова.

Фонд оценочных средств является неотъемлемой частью рабочей программы дисциплины.

Разработчик: О.А. Левичев, к. в. н., доцент

Заведующий кафедрой _____/ Н. Н. Загускин

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

Настоящий Фонд оценочных средств (ФОС) по дисциплине «Информационная безопасность и защита данных» является неотъемлемым приложением к рабочей программе дисциплины (РПД) «Информационная безопасность и защита данных». 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	Курсовая работа	Вид контроля, позволяющий выявить степень владения базовыми знаниями, умениями и навыками, необходимыми для обучения, и определить уровень владения новым материалом	Индивидуальные задания (темы) для курсовой работы
6	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. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ ДИСЦИПЛИНЕ

3.1. Сопроводительная информация.

Разработчик	О.А. Левичев, к. в. н., доцент
Кафедра	информационных технологий и прикладной информатики
Наименование дисциплины	Информационная безопасность и защита данных
Факультет / институт	Международный институт инновационной экономики, лидерства и менеджмента
Направление подготовки / специальность	09.04.03 Прикладная информатика
Количество вопросов в оценочных заданиях (диапазон)	От 15 до 30
Общее время тестирования (мин)	90
Общее количество вопросов/заданий в ФОС	*30*
Размещенность на сайте Университета примерного перечня вопросов, заданий ФОС – для подготовки обучающихся к прохождению оценки (да / нет)	*Да*

3.2. Характеристика оцениваемых компетенций.

Код компетенции	Формулировка компетенции	Индикаторы достижения компетенции
УК-6	Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки	ИУК-6.1. Знает, как проводить самооценку собственной деятельности, определяет сильные стороны, зоны роста и целевые ориентиры развития ИУК-6.2. Умеет определять приоритеты деятельности, планирует ресурсы и выбирает способы совершенствования компетенций с учётом ограничений и контекста ИУК-6.3. Владеет навыками реализации планов совершенствования, контролирует прогресс, корректирует действия и фиксирует результаты для дальнейшего развития
ПК-2	Способен обосновывать выбор моделей данных, методов и инструментальных средств проектирования и разработки баз данных ИС с учётом требований заказчика	ИПК-2.1 Знать: классификацию моделей данных (реляционные, NoSQL, гибридные), методы их сравнительного анализа и современные инструментальные средства проектирования и разработки БД. ИПК-2.2 Уметь: выполнять сравнительный анализ моделей данных и инструментальных средств, формализовать требования заказчика и формировать обоснованные рекомендации по выбору технологий. ИПК-2.3 Владеть: методами обоснования технических решений и инструментальными средствами моделирования БД для апробации и аргументации выбора.

4. СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ТЕКУЩЕГО КОНТРОЛЯ

4.1. ТИПОВЫЕ ТЕСТОВЫЕ ЗАДАНИЯ.

Тесты содержат набор вопросов, в полном объеме охватывающие изученный теоретический материал по указанной теме (индикаторы ЗНАТЬ). Выполнение тестов позволяет определить результат освоения компетенций по дисциплине в рамках рассматриваемой темы, оцениваемый с помощью соответствующих индикаторов достижения компетенций. Индивидуальный тестовый сеанс для каждого обучающегося формируется по специальному алгоритму, обеспечивающему заданную тематическую структуру и пропорциональное наличие вопросов разного типа и сложности.

При формировании тестов необходимо использовать задания следующих типов:

Тип задания 1. Задания закрытого типа на установление соответствия.

Тип задания 2. Задания закрытого типа на установление последовательности.

Тип задания 3. Задания комбинированного типа, предполагающие выбор одного правильного ответа из предложенных с последующим объяснением своего выбора.

Тип задания 4. Задания комбинированного типа, предполагающие выбор нескольких ответов из предложенных с последующим объяснением своего выбора.

Тип задания 5. Задания открытого типа с развернутым ответом.

Тема	**Код и формулировка компетенции**	**Индикаторы достижения компетенции**	**Тест по теме**
Тема. 1 Введение в информационную безопасность	УК-6. Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки	ИУК-6.1. Знает, как проводить самооценку собственной деятельности, определяет сильные стороны, зоны роста и целевые ориентиры развития	1.1. Триада КЦД (CIA) включает: а) конфиденциальность, целостность, доступность; б) контроль, целостность, дублирование; в) качество, целостность, дублирование; г) контроль, целостность, доверие 1.2. Целостность информации означает: а) актуальность данных и защиту от несанкционированного изменения; б) доступность данных в любой момент; в) секретность данных; г) наличие резервных копий 1.3. Аутентификация отличается от идентификации тем, что: а) проверяет, действительно ли субъект тот, за кого себя выдаёт; б) только сообщает имя пользователя; в) распределяет права доступа; г) шифрует данные 1.4. Авторизация — это: а) предоставление субъекту прав на выполнение действий; б) проверка подлинности; в) уничтожение данных; г) регистрация событий
Тема. 2 Законодательный уровень информационной безопасности	УК-6. Способен определять и реализовывать приоритеты собственн	ИУК-6.2. Умеет определять приоритеты деятельности, планирует ресурсы и выбирает способы	1.5. К организационным мерам защиты информации относятся: а) политика безопасности, обучение персонала, режим доступа в помещения; б) только антивирус; б) только межсетевой экран; в) только шифрование дисков; г) только видеонаблюдение 1.5. Принцип наименьших привилегий (least privilege) означает: а) предоставление только тех

	ой деятельности и способы ее совершенствования на основе самооценки	совершенствования компетенций с учётом ограничений и контекста я	прав, которые необходимы для выполнения задачи; б) выдачу максимальных прав всем; в) запрет всех действий; г) единый пароль для отдела 1.6. Угроза информационной безопасности — это: а) потенциально возможное событие или действие, которое может нарушить КЦД информации; б) уже случившееся нарушение; в) любое событие ФСТЭК; 1) вид фишинга
Тема. 3 Стандарты и спецификации в области информационной безопасности	УК-6. Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки	ИУК-6.3. Владеет навыками реализации планов совершенствования, контролирует прогресс, корректирует действия и фиксирует результаты для дальнейшего развити	2.1. Симметричное шифрование использует: а) пару ключей «открытый — закрытый»; б) один и тот же ключ для шифрования и расшифрования; в) только биометрию; г) вообще без ключей 2.2. Асимметричное шифрование (например, RSA) основано на: а) паре ключей: открытый для шифрования/проверки подписи, закрытый для расшифрования/подписи; б) одном общем ключе у всех; в) пароле из 6 символов; г) отсутствии ключей 2.3. Криптографическая хеш-функция (SHA-256) — это: а) обратимое преобразование данных; б) способ сжатия архива; в) необратимое преобразование данных в строку фиксированной длины; г) метод шифрования почты 2.4. Электронная подпись обеспечивает: а) целостность документа, подтверждение авторства и неотказуемость; б) только сжатие файла; в) только ускорение загрузки; г) только шифрование всего диска
Тема. 4 Административный уровень информационной безопасности	УК-6. Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки	ИУК-6.2. Умеет определять приоритеты деятельности, планирует ресурсы и выбирает способы совершенствования компетенций с учётом ограничений и контекста я	2.5. «Соль» при хранении паролей — это: а) метка сервера; б) случайная строка, добавляемая к паролю перед хешированием для защиты от радужных таблиц; в) название алгоритма; г) резервная копия пароля 2.6. Двухфакторная аутентификация (2FA) — это: а) два разных пароля; б) вход с двух компьютеров; в) двойное шифрование; г) пароль плюс независимый второй фактор: одноразовый код, токен, биометрия
Тема. 5 Процедурный	УК-6. Способен определять	ИУК-6.3. Владеет навыками	3.1. Межсетевой экран (firewall) предназначен для: а) фильтрации сетевого трафика по заданным правилам; б) антивирусной защиты почты; в)

уровень информационной безопасности	и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки	реализации планов совершенствования, контролирует прогресс, корректирует действия и фиксирует результаты для дальнейшего развити	сжатия данных; г) раздачи Wi-Fi 3.2. Система предотвращения вторжений (IPS) отличается от IDS тем, что: а) только записывает события; б) активно блокирует обнаруженные атаки, а не только обнаруживает их; в) работает без сети; г) заменяет антивирус на всех ПК 3.3. VPN применяется для: а) ускорения интернета; б) обхода ограничений провайдера; в) создания защищённого туннеля между пользователем и корпоративной сетью; г) печати документов по сети 3.4. SQL-инъекция — это: а) подмена MAC-адреса; б) внедрение вредоносного SQL-кода через пользовательский ввод; в) переполнение буфера; г) фишинговое письмо
Тема. 6 Идентификация и аутентификация	ПК-2. Способен обосновывать выбор моделей данных, методов и инструментальных средств проектирования и разработки баз данных ИС с учётом требований заказчика	И П К - 2 . 1 Знать: классификацию моделей данных (реляционные, NoSQL, гибридные), методы их сравнительного анализа и современные инструментальные средства проектирования и разработки БД.	3.5. DDoS-атака направлена на: а) исчерпание ресурсов системы множеством одновременных запросов, чтобы сделать сервис недоступным; б) кражу паролей администратора; в) изменение базы данных; г) установку вирусов на сервер 3.6. Межсайтовый скриптинг (XSS) — это атака, при которой: а) подбирается пароль по словарю; б) перехватывается Wi-Fi-трафик; в) подменяется DNS-запись; г) в страницу внедряется вредоносный скрипт, исполняемый в браузере жертвы
Тема. 7 Управление доступом. Протоколирование и аудит	ПК-2. Способен обосновывать выбор моделей данных, методов и инструментальных средств проектирования и разработки баз данных ИС с	И П К - 2 . 2 Уметь: выполнять сравнительный анализ моделей данных и инструментальных средств, формализовать требования заказчика и формировать	4.1. Основной закон, регулирующий обработку персональных данных в РФ: а) 187-ФЗ; б) 152-ФЗ «О персональных данных»; в) 149-ФЗ; г) 98-ФЗ «О коммерческой тайне» 4.2. Оператор персональных данных — это: а) сотрудник техподдержки; б) любой посетитель сайта; в) лицо, организующее и осуществляющее обработку персональных данных; г) только государственный орган 4.3. Обезличивание персональных данных — это: а) обработка, в результате которой данные перестают позволять идентифицировать субъект без дополнительной информации; б) удаление всей

	учётом требований заказчика	обоснованные рекомендации по выбору технологий	базы; в) шифрование диска; г) передача данных за границу
Тема. 8 Криптографические методы защиты	ПК-2. Способен обосновывать выбор моделей данных, методов и инструментальных средств проектирования и разработки баз данных ИС с учётом требований заказчика	ИПК-2.3 Владеть: методами обоснования технических решений и инструментальными средствами моделирования БД для апробации и аргументации выбора.	4.4. Согласие субъекта на обработку персональных данных должно быть: а) любым, достаточно молчания; б) конкретным, информированным и сознательным; в) получено задним числом; г) только устным 4.5. Безопасность критической информационной инфраструктуры (КИИ) в РФ регулирует: а) 98-ФЗ; б) 436-ФЗ; в) 149-ФЗ; г) 187-ФЗ 4.6. Обязанность подать уведомление об обработке персональных данных в Роскомнадзор лежит на: а) операторе персональных данных (за исключением случаев, предусмотренных законом); б) пользователях сайта; в) интернет-провайдере; г) налоговой инспекции
Тема. 9 Контроль целостности	ПК-2. Способен обосновывать выбор моделей данных, методов и инструментальных средств проектирования и разработки баз данных ИС с учётом требований заказчика	И П К - 2 . 1 Знать: классификацию моделей данных (реляционные, NoSQL, гибридные), методы их сравнительного анализа и современные инструментальные средства проектирования и разработки БД.	5.1. Правило резервного копирования 3-2-1 означает: а) копию раз в три месяца; б) минимум 3 копии данных, на 2 разных типах носителей, 1 копия — вне основной площадки; в) 3 сервера в одной стойке; г) 2 пароля и 1 логин 5.2. Ролевая модель доступа (RBAC) предполагает, что: а) права назначаются не конкретному человеку, а роли, к которой он привязан; б) все имеют права администратора; в) доступ выдаётся по ФИО; г) права меняются ежедневно 5.3. Журналирование (аудит) событий безопасности нужно для: а) оформления пропусков; б) учёта отработанного времени; в) регистрации действий пользователей и расследования инцидентов; г) ускорения системы
Тема. 10 Экранирование. Тунелирование	ПК-2. Способен обосновывать выбор моделей данных, методов и инструментальных средств	ИПК-2.2 Уметь: выполнять сравнительный анализ моделей данных и инструментальных средств,	5.4. Социальная инженерия — это: а) планирование соцсетей компании; б) получение доступа к информации через обман и психологические манипуляции людьми; в) управление персоналом; г) защита от инсайдеров техническими средствами 5.5. При выявлении утечки персональных данных оператор обязан: а) уведомить Роскомнадзор и принять меры по локализации и устранению

	проектирования и разработки баз данных ИС с учётом требований заказчика	формализовать требования заказчика и формировать обоснованные рекомендации по выбору технологий	последствий; б) удалить пострадавшую базу и молчать; в) уволить дежурного администратора; г) ждать запроса от пострадавших 5.6. Регулярное обучение сотрудников правилам информационной безопасности прежде всего снижает риск: а) поломки жёсткого диска; б) фишинга и социальной инженерии; в) устаревания оборудования; г) роста тарифов на связь
Тема. 11 Анализ защищенности	ПК-2. Способен обосновывать выбор моделей данных, методов и инструментальных средств проектирования и разработки баз данных ИС с учётом требований заказчика	ИПК-2.3 Владеть: методами обоснования технических решений и инструментальными средствами моделирования БД для апробации и аргументации выбора.	6.1. Шифровальщик (ransomware) — это вредоносное ПО, которое: а) собирает статистику браузера; б) показывает рекламу; в) шифрует данные жертвы и требует выкуп за расшифровку; г) рассылает спам 6.2. Zero-day (уязвимость нулевого дня) — это: а) уязвимость, для которой ещё не существует патча и о которой разработчик не знает; б) уязвимость, найденная случайно; в) устаревший антивирус; г) просроченный сертификат 6.3. Ботнет — это: а) бот-ассистент в мессенджере; б) сеть заражённых устройств, управляемая злоумышленником (часто для DDoS-атак и рассылок); в) автоматический ответчик на почте; г) название антивируса 6.4. Пентест (тестирование на проникновение) — это: а) авторизованная проверка защищённости системы методами реального злоумышленника; б) несанкционированный взлом чужой сети; в) нагрузочное тестирование сервера; г) проверка расписания дежурств 6.5. Концепция Zero Trust («нулевое доверие») предполагает: а) доверие ко всему внутреннему трафику; б) отказ от паролей; в) отключение межсетевого экрана; г) проверку каждого запроса независимо от источника: «никому не доверяй, всегда проверяй»

Критерии оценивания диагностической работы:

Оценка	Критерии оценивания
отлично	от 90 до 100 % правильно выполненных заданий
хорошо	от 70 до 89 % правильно выполненных заданий
удовлетворительно	от 50 до 69 % правильно выполненных заданий
неудовлетворительно	менее 50 % правильно выполненных заданий