

**Федеральное государственное бюджетное учреждение науки
Институт машиноведения им. А.А. Благонравова
Российской академии наук
(ИМАШ РАН)**

УТВЕРЖДАЮ
Заместитель директора по вопросам
подготовки кадров высшей
квалификации ИМАШ РАН
к.ф.-м.н. Жданов Э.Р.
« 01 » _____ 2026 года
М.П.



**Комплект оценочных материалов
по дисциплине «Основы информационной безопасности»**

Направление подготовки:	09.04.03 Прикладная информатика
Профиль подготовки:	Цифровые двойники и автоматизированные системы управления технологическими процессами
Квалификация:	Магистр
Форма обучения	Очная

Содержание

1. Общие положения.....	3
2. Результаты освоения дисциплины, подлежащие проверке.....	3
3. Контроль и оценка освоения учебной дисциплины.....	4
4. Оценочные материалы для проведения текущего контроля успеваемости.....	4
5. Оценочные материалы для проведения промежуточной аттестации.....	7

1. Общие положения

Комплект оценочных материалов (далее - ОМ) предназначен для контроля и оценки образовательных достижений обучающихся, освоивших программу дисциплины «Основы информационной безопасности».

ОМ включают контрольные материалы для проведения текущего контроля успеваемости и промежуточной аттестации в форме экзамена.

ОМ разработаны на основании:

- основной профессиональной образовательной программы по направлению подготовки 09.04.03 Прикладная информатика;
- рабочей программы дисциплины «Основы информационной безопасности».

2. Результаты освоения дисциплины, подлежащие проверке

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями

ОПК-5	Способен разрабатывать и модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем
ОПК-5.1	Знает современное программное и аппаратное обеспечение информационных и автоматизированных систем
ОПК-5.2	Умеет модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем для решения профессиональных задач

Код индикатора компетенции	Планируемые результаты обучения по дисциплине
ОПК-5.1	<i>Знать:</i> - архитектуру и состав современных программно-аппаратных комплексов, используемых в информационных системах и автоматизированных системах управления технологическими процессами (АСУ ТП); - принципы работы и особенности аппаратных платформ (контроллеры, серверы, IoT-устройства) и системного программного обеспечения, применяемого для построения цифровых двойников и промышленных сетей. <i>Уметь:</i> - идентифицировать и классифицировать основные компоненты программно-аппаратного обеспечения информационной системы; - анализировать технические характеристики аппаратных средств и программного окружения для оценки их применимости в задачах промышленной автоматизации. <i>Иметь практический опыт:</i> - работы с современными образцами аппаратного обеспечения (контроллеры, модули ввода-вывода, сетевое оборудование) и их настройки в составе лабораторных стендов; - установки, конфигурирования и диагностики операционных систем и специализированного ПО, используемого в АСУ ТП.
ОПК-5.2	<i>Знать:</i> - методы и технологии модернизации аппаратных платформ и программного обеспечения, включая обновление микропрограмм (firmware), драйверов и системного ПО для обеспечения совместимости и повышения производительности; - принципы обратной совместимости и миграции данных при обновлении компонентов автоматизированных систем управления. <i>Уметь:</i> - планировать и реализовывать мероприятия по модернизации аппаратного и программного обеспечения с учётом требований информационной безопасности и непрерывности производственного процесса; - выполнять установку, настройку и интеграцию новых версий ПО и

	оборудования в существующую инфраструктуру АСУ ТП. <i>Иметь практический опыт:</i> - проведения апгрейда аппаратных компонентов (например, замена контроллеров, модулей ввода-вывода) на лабораторных стендах или в симулированной среде; - обновления версий системного и прикладного ПО, а также драйверов устройств в составе автоматизированной системы.
--	---

3. Контроль и оценка освоения учебной дисциплины

Элемент учебной дисциплины	Текущий контроль		Промежуточная аттестация	
	Форма контроля	Проверяемые идк	Форма контроля	Проверяемые идк
Тема 1. Введение в информационную безопасность	Отчет по лабораторному практикуму Практикум по решению задач	ОПК-5.1 ОПК-5.2		
Тема 2. Угрозы и уязвимости в АСУ ТП и цифровых двойников	Отчет по лабораторному практикуму Практикум по решению задач	ОПК-5.1 ОПК-5.2		
Тема 3. Методы и средства защиты информации	Отчет по лабораторному практикуму Практикум по решению задач	ОПК-5.1 ОПК-5.2		
Тема 4. Управление информационной безопасностью	Отчет по лабораторному практикуму Практикум по решению задач	ОПК-5.1 ОПК-5.2		
Тема 5. Практические аспекты обеспечения ИБ в цифровых двойниках	Отчет по лабораторному практикуму Практикум по решению задач	ОПК-5.1 ОПК-5.2		
			Экзамен	ОПК-5.1 ОПК-5.2

4. Оценочные материалы для проведения текущего контроля успеваемости

Показатели и критерии оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Лабораторный практикум
10 -8 – работа выполнена в срок, самостоятельно, правильно поняты и использованы соответствующие формулы, правильно определены соответствующие спецификации, использована требуемая информация, правильно выполнены требуемые расчеты, правильно выбраны совместимые комплектующие, сделаны необходимые выводы, хорошо аргументированы, даны исчерпывающие ответы на все поставленные вопросы 7- 5– работа выполнена в срок, самостоятельно, правильно поняты и использованы соответствующие формулы, правильно определены соответствующие спецификации, использована требуемая информация, правильно выполнены требуемые расчеты, правильно

выбраны совместимые комплектующие, необходимые выводы сделаны частично, хорошо аргументированы, даны ответы на все поставленные вопросы
4-3 – работа выполнена в срок, в основном самостоятельно, использованы соответствующие формулы; определены соответствующие спецификации, имеются ошибки в расчетах; выбраны совместимые комплектующие необходимые, выводы сделаны частично, слабо аргументированы, даны ответы не на все вопросы
2-1 – обучающийся подготовил работу несамостоятельно или не завершил в срок, описание спецификации содержит незначительные ошибки, выводы и ответы на вопросы отсутствуют.

Практикум по решению задач

10-8 – работа и отчет выполнены в срок, самостоятельно, правильно определены соответствующие спецификации, использована требуемая информация, правильно выполнены требуемые расчеты, сделаны необходимые выводы, хорошо аргументированы, даны исчерпывающие ответы на все поставленные вопросы;
7-5– работа и отчет выполнены в срок, самостоятельно, правильно определены соответствующие спецификации, использована требуемая информация, правильно выполнены требуемые расчеты, необходимые выводы сделаны частично, хорошо аргументированы, даны ответы на все поставленные вопросы;
4-1 – работа и отчет выполнены в срок, в основном самостоятельно, выводы сделаны частично, слабо аргументированы, даны ответы не на все вопросы;
0 – обучающийся подготовил работу и отчет несамостоятельно и/или не завершил в срок, описание содержит ошибки, выводы и ответы на вопросы отсутствуют.

Порядок начисления баллов

Если студент набрал достаточное количество баллов ТКУ по дисциплине (более 70 баллов) в течение семестра, он может отказаться от сдачи экзамена, и результат будет выставлен автоматически по его согласию.

Типовые контрольные задания и иные материалы, необходимые для процедуры оценивания знаний, умений, навыков и(или) опыта деятельности

Типовые задания практикумов по решению задач

Тема 1. Введение в информационную безопасность

Задача 1.

Анализ кейса: Дана краткая характеристика информационной системы предприятия (например, «Машиностроительный завод»). Требуется определить основные активы (информационные и технические), для которых необходимо обеспечить конфиденциальность, целостность и доступность. Сформулировать цели ИБ для данного предприятия.

Задача 2.

Классификация угроз: Составить перечень из 10 потенциальных угроз для информационной системы малого производственного цеха. Классифицировать их по источнику (антропогенные/техногенные) и преднамеренности (случайные/преднамеренные).

Тема 2. Угрозы и уязвимости в АСУ ТП и цифровых двойниках

Задача 1.

Моделирование нарушителя: Для заданной системы (например, автоматизированная линия розлива) разработать модель внутреннего нарушителя (оператор смены). Описать его потенциальные возможности, мотивацию и сценарий атаки.

Задача 2.

Анализ уязвимостей. На основе описания промышленной сети (топология, используемое оборудование: ПЛК, сервер SCADA) выявить не менее 5 потенциальных уязвимостей (например, отсутствие сегментации сети, использование стандартных паролей) и предложить меры по их устранению.

Тема 3. Методы и средства защиты информации

Задача 1.

Выбор средства защиты: Для сценария «Подключение удаленного филиала к корпоративной сети» выбрать и обосновать тип межсетевого экрана (NGFW/UTM), описать необходимые правила фильтрации трафика.

Задача 2.

Проектирование криптозащиты: Описать схему применения электронной подписи для обеспечения целостности и авторства технологической инструкции, передаваемой от инженера-технолога к оператору на АРМ.

Тема 4. Управление информационной безопасностью

Задача 1.

Разработка фрагмента политики ИБ: Написать раздел «Политика использования паролей» для организации. Требования должны включать минимальную длину, сложность, срок действия пароля.

Задача 2.

Планирование реагирования на инцидент: Разработать первичный план действий для системного администратора при обнаружении факта заражения рабочей станции вирусом-шифровальщиком.

Раздел 5. Практические аспекты обеспечения ИБ в цифровых двойниках

Задача 1.

Обеспечение достоверности данных. Предложить метод (технический или организационный) проверки того, что данные, поступающие от физического датчика температуры в цифровой двойник, не были преднамеренно искажены злоумышленником.

Задача 2.

Управление доступом: Разработать матрицу доступа для цифрового двойника производственной линии. Роли: «Технолог», «Инженер по ремонту», «Аналитик», «Системный администратор». Определить права доступа (чтение/запись) к данным телеметрии, моделям, историческим данным.

Типовые задания для лабораторных практикумов

Тема 1. Введение в информационную безопасность

Работа с нормативной базой.

Используя правовые системы («КонсультантПлюс», «Гарант»), найти и проанализировать основные статьи Федерального закона № 187-ФЗ «О безопасности критической информационной инфраструктуры РФ». Составить краткую справку о требованиях к субъектам КИИ.

Тема 2. Угрозы и уязвимости в АСУ ТП и цифровых двойниках

Исследование трафика (в виртуальной среде): Используя анализатор трафика (например, Wireshark), изучить дампы сетевого обмена между компонентами АСУ ТП. Идентифицировать используемые протоколы (например, Modbus TCP), найти пакеты с данными и оценить возможность их перехвата в незашифрованном виде.

Тема 3. Методы и средства защиты информации

Настройка межсетевого экрана: В виртуальной лаборатории (GNS3, EVE-NG) развернуть стенд из двух сегментов («Офис» и «Производство») и настроить правила на виртуальном межсетевом экране (pfSense, VyOS) для разрешения доступа к веб-серверу из офиса и блокировки всех остальных соединений из производственного сегмента.

Генерация ключевой пары: С помощью утилиты OpenSSL (или аналога) создать пару ключей (открытый/закрытый), сформировать самоподписанный сертификат и

выполнить операции шифрования и расшифрования короткого текстового файла.

Тема 4. Управление информационной безопасностью

Анализ логов: В предоставленном текстовом файле (имитация системного журнала) найти записи, свидетельствующие о подозрительной активности (например, многократные неудачные попытки входа под учетной записью администратора, сканирование портов). Сформулировать гипотезу о типе атаки.

Раздел 5. Практические аспекты обеспечения ИБ в цифровых двойниках

Симуляция атаки «Человек посередине» (MitM): В изолированной виртуальной сети продемонстрировать перехват и модификацию данных, передаваемых между симулятором физического объекта и его цифровой моделью, при отсутствии средств защиты (шифрования). Затем реализовать простую защиту (например, TLS-туннель) и показать невозможность модификации данных.

5. Оценочные материалы для проведения промежуточной аттестации

Промежуточная аттестация по дисциплине проводится в форме экзамена.

Экзамен представляет собой выполнение обучающимся заданий билета, включающего в себя:

Задание №1 – теоретический вопрос на знание базовых понятий предметной области дисциплины, а также позволяющий оценить степень владения обучающегося принципами предметной области дисциплины, понимание их особенностей и взаимосвязи между ними.

Задание №2 – задание на анализ ситуации из предметной области дисциплины и выявление способности обучающегося выбирать и применять соответствующие принципы и методы решения практических проблем, близких к профессиональной деятельности.

Задания №3 – задания на проверку умений и навыков, полученных в результате освоения дисциплины.

Выполнение обучающимся заданий билета оценивается по следующей балльной шкале:

Задание 1: 0-30 баллов

Задание 2: 0-30 баллов

Задание 3: 0-40 баллов

- **90 и более (отлично)** – ответ правильный, логически выстроен, приведены необходимые выкладки, использована профессиональная лексика. Задания решены правильно. Обучающийся правильно интерпретирует полученный результат.

- **89-70 (хорошо)**– ответ в целом правильный, логически выстроен, приведены необходимые выкладки, использована профессиональная лексика. Ход решения задания правильный, ответ неверный. Обучающийся в целом правильно интерпретирует полученный результат.

- **69-50 (удовлетворительно)**– ответ в основном правильный, логически выстроен, приведены не все необходимые выкладки, использована профессиональная лексика. Задания решены частично.

- **менее 50 (неудовлетворительно)**– ответы на теоретическую часть неправильные или неполные. Задания не решены.

Типовые задания для проведения промежуточной аттестации обучающихся

Задания 1-го типа

1. Дайте определение информационной безопасности. Раскройте содержание классической триады CIA (конфиденциальность, целостность, доступность) и проиллюстрируйте её примерами применительно к данным цифрового двойника и командам управления в АСУ ТП.

2. Что такое критическая информационная инфраструктура (КИИ)? Перечислите основные категории объектов КИИ в промышленности и назовите ключевые положения Федерального закона № 187-ФЗ, регулирующего их безопасность.
3. Проведите сравнительный анализ угроз информационной безопасности для классических корпоративных сетей и для автоматизированных систем управления технологическими процессами (АСУ ТП). В чём заключается их принципиальное различие?
4. Опишите модель нарушителя во внутренней сети АСУ ТП (модель «инсайдера»). Каковы его потенциальные возможности и типичные векторы атак на технологический процесс?
5. Что такое «цифровой двойник» с точки зрения информационной безопасности? Каковы основные угрозы целостности и доступности данных, связывающих физическую установку и её виртуальную модель?
6. Дайте определение уязвимости. Приведите примеры программных (уязвимости в SCADA) и аппаратных (уязвимости в ПЛК) уязвимостей, характерных для промышленных систем.
7. Объясните принцип работы межсетевого экранирования (Firewalling). Почему простая маршрутизация трафика между корпоративным и технологическим сегментами сети является недопустимой с точки зрения ИБ?
8. Что такое системы обнаружения/предотвращения вторжений (IDS/IPS)? В чём заключается специфика IDS/IPS для промышленных протоколов (например, Modbus, Profinet) по сравнению с системами для IP-сетей?
9. Раскройте понятие «сегментация сети» в контексте защиты АСУ ТП. Опишите типовую архитектуру с разделением на зоны (например, корпоративная сеть, DMZ, технологическая сеть) и уровни управления.
10. Какова роль криптографии в обеспечении безопасности АСУ ТП? Сравните задачи, решаемые с помощью симметричного шифрования и электронной подписи в промышленных системах.
11. Опишите жизненный цикл инцидента информационной безопасности. Каковы особенности реагирования на инциденты в действующих АСУ ТП, где остановка системы недопустима?
12. Что такое аудит информационной безопасности? Какие виды аудита (внутренний, внешний, compliance) применяются для проверки систем управления производством и каковы их цели?
13. Дайте определение политики информационной безопасности. Какие ключевые разделы должна содержать политика ИБ для предприятия с автоматизированным производством?
14. Объясните концепцию «Планирования непрерывности бизнеса» (BCP) и «Аварийного восстановления» (DRP). Почему для АСУ ТП план DRP имеет критическое значение и чем он отличается от аналогичного плана для офиса?
15. Что такое управление доступом? Опишите ролевую модель доступа (RBAC) применительно к пользователям цифрового двойника (инженер, оператор, аналитик).
16. Раскройте понятие «человеческий фактор» как угрозы ИБ. Приведите примеры методов социальной инженерии, направленных на персонал, обслуживающий АСУ ТП.
17. Что такое управление обновлениями (Patch Management)? С какими рисками и сложностями сопряжено обновление ПО на работающих контроллерах (ПЛК) в реальном производстве?
18. Дайте определение модели угроз и модели нарушителя. Какова последовательность действий при разработке модели угроз для конкретного производственного объекта?
19. Опишите принцип работы систем мониторинга событий безопасности (SIEM). Какую роль играет централизованный сбор логов с компонентов АСУ ТП для выявления аномалий и расследования инцидентов?

20. Каковы основные принципы обеспечения безопасности на различных этапах жизненного цикла цифрового двойника (проектирование, внедрение, эксплуатация, вывод из эксплуатации)?

Задания 2-го типа

1. Ситуация: На заводе оператор АРМ заметил резкое замедление работы SCADA-системы, а затем самопроизвольное изменение уставки температуры в реакторе. Опишите ваши первые действия как специалиста по ИБ и гипотезу о типе атаки.

2. Ситуация: Руководство требует предоставить удалённый доступ к системе мониторинга производства для топ-менеджмента через интернет. Опишите безопасный способ реализации этого доступа, включая выбор технологий (например, VPN) и архитектуру.

3. Ситуация: В ходе планового сканирования сети обнаружен ПЛК с заводским паролем по умолчанию. Производство остановить невозможно. Предложите пошаговый план действий по устранению уязвимости с минимальными рисками.

4. Ситуация: Произошёл сбой основного сервера SCADA. Из резервной копии (бэкапа) данные не восстанавливаются. Опишите, как принципы BCP/DRP должны были предотвратить эту ситуацию и ваши действия по восстановлению контроля над процессом.

5. Ситуация: Служба мониторинга зафиксировала передачу большого объёма данных с сегмента сети АСУ ТП на внешний IP-адрес в ночное время. Опишите алгоритм расследования инцидента и методы анализа трафика для выявления источника утечки.

6. Ситуация: Необходимо обновить прошивку (firmware) на 50 распределённых контроллерах. Опишите процедуру обновления с точки зрения ИБ, минимизирующую риски отказа оборудования и внедрения вредоносного кода.

7. Ситуация: В системе управления обнаружен вирус-шифровальщик. Критически важные процессы управления не затронуты, но база данных истории параметров зашифрована. Ваши действия по локализации угрозы и восстановлению данных?

8. Ситуация: Инженер-технолог хочет подключить к технологической сети свой личный ноутбук для анализа данных. Опишите, какие технические (настройка Firewall) и организационные (политика ИБ) меры необходимо применить.

9. Ситуация: При аудите обнаружено, что на сервере архивации (Historian) открыт доступ к порту 445 (SMB) из корпоративной сети. Оцените риск и опишите, как изменить конфигурацию межсетевого экрана для устранения угрозы.

10. Ситуация: Необходимо разработать политику паролей для операторов АСУ ТП. Учтите, что операторы работают в сменном режиме 24/7. Сформулируйте требования к сложности и смене паролей, балансируя между безопасностью и удобством эксплуатации.

11. Ситуация: Подрядчик для настройки оборудования требует временного подключения к сегменту управления через свой ноутбук. Опишите процедуру безопасного подключения (например, через VDI или изолированный сегмент) и контроля его действий.

12. Ситуация: В логах межсетевого экрана зафиксированы множественные попытки подбора пароля (Brute-force) к SSH-сервису на сервере сбора данных. Опишите методы противодействия (технические настройки сервера и правила IPS).

13. Ситуация: Выявлена критическая уязвимость в протоколе передачи данных между физическим датчиком и цифровым двойником. Как обеспечить целостность данных «здесь и сейчас», пока не будет обновлено ПО?

14. Ситуация: После увольнения системного администратора выяснилось, что его учётная запись с правами доступа ко всем серверам всё ещё активна. Опишите, как должна быть выстроена процедура управления учётными записями (Identity Management), чтобы исключить такие ситуации.

15. Ситуация: Необходимо передать проектную документацию цифрового двойника (включая математические модели) внешнему подрядчику. Как обеспечить конфиденциальность этой информации при передаче?

16. Ситуация: В технологической сети используется устаревшее оборудование,

которое не поддерживает современные протоколы шифрования, но его замена стоит миллионы долларов. Предложите компенсирующие меры защиты для этого сегмента сети.

17. Ситуация: Оператор случайно ввёл команду на остановку конвейера, приняв фишинговое письмо за уведомление от системы. Опишите комплекс мер (технические и обучение персонала), которые могли бы предотвратить этот инцидент.

18. Ситуация: Служба ИБ требует установить антивирус на ПЛК. Инженер АСУ ТП утверждает, что это невозможно и опасно для реального времени. Кто прав? Предложите альтернативный метод защиты контроллера от вредоносного ПО.

19. Ситуация: Необходимо провести аудит защищённости работающей АСУ ТП без остановки производства. Опишите методы «пассивного» аудита (анализ конфигурации, трафика) и границы его применимости.

20. Ситуация: В результате сбоя питания сервер цифрового двойника некорректно завершил работу, и база данных оказалась повреждена. Опишите роль систем резервного копирования и репликации в обеспечении доступности цифрового двойника.

Задания 3-го типа

Задание 1. Анализ правил межсетевого экрана

Ситуация: Вам предоставлен список из 10 правил межсетевого экрана (в текстовом виде или скриншот интерфейса pfSense/VyOS) для защиты сегмента АСУ ТП.

Задача: Найти в списке как минимум 3 некорректных или небезопасных правила. Объяснить, какую угрозу создаёт каждое из них, и предложить исправленный вариант правила.

Задание 2. Разработка матрицы доступа (RBAC)

Ситуация: Для цифрового двойника производственной линии определены три роли: «Оператор» (только просмотр), «Технолог» (просмотр и изменение параметров), «Аналитик» (только чтение исторических данных).

Задача: Составить простую таблицу (матрицу), где по строкам указаны ресурсы (данные датчиков, уставки, история), а по столбцам — права доступа (R, W) для каждой роли.

Задание 3. Идентификация атаки по логам

Ситуация: Вам предоставлен фрагмент системного журнала (лога) веб-сервера или межсетевого экрана.

Задача: Проанализировать лог и определить, какой тип атаки зафиксирован (например, SQL-инъекция, Brute-force, сканирование портов). Описать признаки, по которым вы сделали вывод.

Задание 4. Проектирование защищенного удаленного доступа

Ситуация: Инженеру необходимо подключиться к системе мониторинга из дома для устранения аварии.

Задача: Описать последовательность технических шагов для организации безопасного подключения. Указать, какие технологии (например, Site-to-Site VPN, RDP через шлюз) и настройки (сложные пароли, двухфакторная аутентификация) должны быть использованы.

Задание 5. Устранение уязвимости «Заводской пароль»

Ситуация: Сканер уязвимостей обнаружил контроллер с учетной записью admin и паролем 12345.

Задача: Составить пошаговый план действий по смене пароля. План должен включать: 1) подготовку (создание бэкапа конфигурации), 2) процедуру смены, 3) проверку работоспособности, 4) документирование.

Задание 6. Классификация инцидента

Ситуация: Описана ситуация: «В технологической сети обнаружен компьютер, рассылающий спам».

Задача: Классифицировать данный инцидент по типу (например, заражение вредоносным ПО). Описать первые три шага по реагированию на инцидент согласно плану

IRP.

Задание 7. Обоснование мер защиты (Кейс)

Ситуация: Руководство считает, что антивирус на серверах АСУ ТП замедляет работу и не нужен, так как они изолированы.

Задача: Написать короткое обоснование (3-4 предложения) для руководства, почему антивирусная защита необходима, и предложить решение, минимизирующее влияние на производительность (например, настройка исключений для процессов).

Задание 8. Разработка политики паролей

Ситуация: Необходимо создать требования к паролям для учетных записей операторов.

Задача: Сформулировать 4-5 конкретных технических требований к паролю (длина, сложность) и правилам его использования (срок действия, история), которые обеспечат баланс между безопасностью и удобством для сменного персонала.

Задание 9. Выбор средства защиты

Ситуация: Требуется защитить веб-интерфейс HMI-панели, доступный из корпоративной сети.

Задача: Выбрать между двумя вариантами: 1) Разместить панель в DMZ за Reverse Proxy. 2) Открыть прямой доступ к панели через Firewall. Обосновать выбор первого варианта с точки зрения безопасности.

Задание 10. Анализ топологии сети

Ситуация: Вам предоставлена схема сети, где сервер базы данных (Historian) находится в одном сегменте с рабочими станциями пользователей корпоративной сети.

Задача: Нарисовать (схематично) исправленную топологию с использованием сегментации (VLAN/подсети) и межсетевого экрана. Объяснить, как это изменение повышает безопасность.