ООО «ИНСТИТУТ ПОВЫШЕНИЯ КВАЛИФИКАЦИИ ГЛАВПРО»

Обучающий центр дополнительного профессионального образования

ТЕХНИЧЕСКАЯ ДОКУМЕНТАЦИЯ

Описание функциональных характеристик программного обеспечения

Платформа обучения информационной безопасности: назначение, состав подсистем, роли и разграничение доступа, сквозные процессы, архитектура, модель данных, технические требования, безопасность, ограничения

Наименование программы	**Платформа обучения информационной безопасности**
Сведения о программе опубликованы	**https://xn--80aeb6arfh.xn--p1ai**
Класс программного обеспечения	**12.17 Программное обеспечение для решения отраслевых задач в области образования**
Тип поставки	**Веб-приложение, устанавливаемое в контуре эксплуатирующей организации**
Язык интерфейса	**Русский**
Дата	**08.10.2026**
Редакция	**1.3**

Назначение документа

Документ описывает функциональные характеристики программного обеспечения в объёме, достаточном для сопровождения и доработки системы техническим специалистом, не участвовавшим в её создании, а также для представления сведений о

программном обеспечении в составе документации, прилагаемой к заявлению о включении сведений в единый реестр российских программ для электронных вычислительных машин и баз данных.

Документ описывает реализованное состояние продукта. Функции, предусмотренные проектными материалами, но не реализованные, а также функции, работоспособность которых зависит от внешних условий, перечислены в разделе 9 и не описаны как действующие.

Оглавление

1 Назначение и область применения
1.1 Решаемая задача
1.2 Пользователи системы
1.3 Контур эксплуатации
1.4 Термины и обозначения
2 Функциональные характеристики
2.1 Состав подсистем
2.2 Управление курсами и их версиями
2.3 Темы и вложения
2.4 Банк вопросов и параметры проверки знаний
2.5 Назначение обучения вручную и по правилам
2.6 Циклы переаттестации и сроки
2.7 Изучение материалов и подтверждение ознакомления
2.8 Тестирование
2.9 Сертификаты и протоколы проверки знаний
2.10 Отчётность и выгрузки
2.11 Имитационные фишинговые рассылки
2.12 Уведомления
2.13 Журналирование
2.14 Справочники, учётные записи, личный кабинет
3 Роли и разграничение доступа
3.1 Роли
3.2 Права доступа
3.3 Уровни проверки прав
3.4 Разграничение на уровне данных
4 Сквозные процессы
4.1 Жизненный цикл курса

4.2 Жизненный цикл назначения обучения

4.3 Изучение материалов и подтверждение ознакомления

4.4 Проверка знаний и выдача сертификата

4.5 Кампания имитационной рассылки

5 Архитектура

5.1 Слои приложения

5.2 Размещение бизнес-логики

5.3 Фоновые задачи и очереди

5.4 Хранение файлов

5.5 Кэширование

6 Модель данных

6.1 Сущности и их назначение

6.2 Связи между сущностями

6.3 Решения, защищающие данные

7 Технические характеристики и требования

7.1 Языки, среды исполнения, библиотеки

7.2 Требования к серверу

7.3 Требования к рабочему месту пользователя

7.4 Показатели производительности

8 Безопасность

9 Ограничения и известные особенности

1. Назначение и область применения

1.1. Решаемая задача

Программное обеспечение представляет собой веб-платформу управления корпоративным обучением в области информационной безопасности и смежных дисциплин. Платформа решает две задачи, связанные между собой, но не сводимые одна к другой.

Организация обучения. Обучающий центр создаёт курсы, наполняет их темами и вложениями, формирует банк проверочных вопросов, назначает обучение работникам вручную или по правилам, задаёт сроки прохождения и периодичность повторного обучения, контролирует ход и результаты.

Формирование доказательств. Платформа фиксирует, что обучение и проверка знаний состоялись, в форме, пригодной для предъявления: протоколов проверки знаний, отметок об ознакомлении с материалом, сертификатов с проверяемым регистрационным номером и неизменяемого журнала юридически значимых событий. Именно эта задача определяет большинство проектных решений, описанных далее, — неизменяемость опубликованных версий курсов, привязку результатов к версии материала, хранение контрольных сумм содержимого и запрет физического удаления данных, на которые опираются результаты.

Обе задачи решаются в отношении одной организации. Разделение по организациям-арендаторам не поддерживается: работники образуют единый список учётных записей, а группировка обеспечивается справочниками подразделений и должностей.

1.2. Пользователи системы

Категория	Задачи в системе	Характер работы
Администратор обучающего центра	Ведение курсов, публикация версий, назначение обучения, ведение справочников, отзыв сертификатов, просмотр неизменяемого журнала, запуск имитационных рассылок, ведение учётных записей и ролей, изменение системных настроек и интеграций, просмотр операционного журнала	Регулярная работа в административной части, преимущественно с настольного рабочего места

Менеджер обучения	Подготовка содержимого курсов, ведение банка вопросов, назначение обучения, контроль результатов, ведение учётных записей работников, просмотр операционного журнала	Работа в административной части без права публикации версий, ведения справочников подразделений и должностей, просмотра неизменяемого журнала, управления ролями и системными настройками
Обучаемый работник	Изучение назначенных материалов, подтверждение ознакомления, прохождение проверки знаний, просмотр собственных результатов и сертификатов	Эпизодическая работа, в том числе с мобильного устройства
Проверяющее лицо	Проверка подлинности предъявленного сертификата по регистрационному номеру	Разовое обращение к общедоступной странице проверки без учётной записи

1.3. Контур эксплуатации

Платформа предназначена для установки в контуре эксплуатирующей организации. Форма поставки — исходный код: образы контейнеров собираются на месте установки из этого кода, а не поставляются в готовом виде (раздел 4.1 инструкции по установке). Все компоненты, необходимые для работы, — сервер приложения, база данных, объектное хранилище, сервер очередей, почтовый шлюз, средство сбора ошибок — разворачиваются внутри контура и не требуют обращения к внешним сетям в ходе работы.

Отсутствие внешних зависимостей обеспечено не только организационно, но и техническими средствами. Статические ресурсы — шрифты, наборы значков, стили, скрипты, включая визуальный редактор содержимого, — поставляются в составе сборки и не загружаются со сторонних узлов. Политика безопасности содержимого, устанавливаемая приложением на каждый ответ, задаёт директивы `default-src 'self'` и `connect-src 'self'`, то есть обращение страницы к постороннему узлу блокируется браузером. Загрузчик набора значков дополнительно возвращает пустое значение вместо обращения к сетевому интерфейсу поставщика значков.

Печатные формы — сертификаты, протоколы проверки знаний, организационные документы — формируются на сервере библиотекой, входящей в поставку; обращения к внешним службам преобразования при этом не выполняются.

Функции, зависящие от внешней инфраструктуры

Перечень исчерпывающий:

- push-уведомления в браузер — доставляются по стандарту Web Push через службы производителей браузеров; функция дополнительная и включается настройкой, при её отключении уведомления доставляются электронной почтой и отображаются внутри интерфейса (раздел 9);
- проверка паролей по перечню утечек — по умолчанию выключена;
- обновление баз антивируса ClamAV (опциональная служба) — с зеркала обновлений в Российской Федерации, которое обеспечивает эксплуатирующая организация;
- загрузка образов контейнеров и пакетов при установке и обновлении.

1.4. Термины и обозначения

Термин	Значение
Курс	Единица обучения, назначаемая работнику. Содержит параметры проверки знаний, периодичность и срок действия результата. Содержимое хранится не в самом курсе, а в его версиях
Версия курса	Снимок содержимого — тем, вложений, вопросов и вариантов ответа. Опубликованная версия неизменяема
Тема (урок)	Раздел учебного материала внутри версии: заголовок, форматированное содержимое, вложения, минимальное время изучения
Назначение	Факт выдачи работнику курса на один цикл обучения. Хранит статус, сроки, номер цикла и зафиксированную версию
Цикл обучения	Одно прохождение курса работником. Нумеруется в пределах пары «работник — курс». Прогресс, попытки и сертификаты относятся к конкретному циклу
Попытка	Один сеанс проверки знаний со своим составом вопросов, таймером и результатом
Подтверждение ознакомления	Действие работника, фиксирующее факт изучения темы вместе с обстоятельствами: временем, сетевым адресом, признаком программы просмотра, контрольной суммой содержимого и текстом формулировки согласия
Неизменяемый журнал	Журнал юридически значимых событий, записи которого связаны хеш-цепочкой и защищены от изменения и удаления средствами базы данных

2. Функциональные характеристики

2.1. Состав подсистем

Подсистема	Назначение	Основные пользователи
Курсы и версии	Ведение перечня курсов, работа с черновиками и публикация версий содержимого	Администратор, менеджер обучения
Темы и вложения	Наполнение версии учебным материалом, загрузка документов, изображений и видеозаписей	Администратор, менеджер обучения
Банк вопросов и параметры проверки знаний	Ведение вопросов и вариантов ответа, настройка порога, числа попыток, таймера и выборки	Администратор, менеджер обучения
Назначение обучения	Выдача курсов работникам вручную, массово и по правилам	Администратор, менеджер обучения
Циклы и сроки	Открытие циклов переаттестации, перевод назначений в просроченные и истёкшие	Выполняется системой по расписанию
Изучение и подтверждение ознакомления	Последовательное изучение тем, учёт времени, фиксация подтверждений	Обучаемый
Проверка знаний	Допуск к тестированию, проведение попытки, подсчёт результата, разбор ответов	Обучаемый
Сертификаты и протоколы	Выдача, отзыв и проверка подлинности сертификатов, формирование протоколов проверки знаний	Администратор, обучаемый, проверяющее лицо
Отчётность	Сводные показатели, списки результатов с фильтрами, детализация, диаграммы, выгрузки	Администратор, менеджер обучения
Имитационные фишинговые рассылки	Шаблоны писем, кампании, фиксация реакции работников, обучающая страница, назначение микрокурса	Администратор, менеджер обучения
Уведомления	Оповещение о назначениях, сроках, результатах и переаттестации по нескольким каналам	Все категории

Журналирование	Операционный журнал изменений и неизменяемый журнал юридически значимых событий	Администратор
Справочники и учётные записи	Подразделения, должности, пользователи, роли, профиль, параметры уведомлений	Администратор

2.2. Управление курсами и их версиями

Перечень курсов

Раздел административной части отображает список курсов с поиском по наименованию, фильтрами по типу, состоянию публикации и признаку архивной записи, а также с постраничной навигацией. Для каждого курса видны тип, состояние, номер действующей версии и число назначений.

Курс имеет один из двух типов, определяющих его поведение на всём протяжении работы:

Тип	Состав	Условие завершения
Обучение	Учебные материалы и проверка знаний	Успешно пройденная попытка проверки знаний
Ознакомление	Только учебные материалы, вопросы недопустимы	Подтверждение ознакомления со всеми активными темами версии

Тип «ознакомление» предназначен для доведения до работников локальных нормативных актов, памяток и инструкций, когда требуется зафиксировать факт ознакомления, а проверка знаний не предусмотрена. Обращение к странице проверки знаний по такому курсу отклоняется с пояснением.

Версии

Содержимое курса хранится не в самом курсе, а в его версиях. Такое разделение введено потому, что результат обучения должен сохранять связь с тем материалом, который работник фактически изучал, даже если материал впоследствии переписан.

Правка содержимого начинается с создания черновика. Черновик получает полную копию содержимого действующей версии — темы, вложения, вопросы и варианты ответа. Файлы вложений при этом физически не копируются: копии ссылаются на те же объекты хранилища, поскольку содержимое файла неизменно и одинаково для обеих версий. Одновременно у курса может существовать не более одного черновика; попытка создать второй отклоняется.

Публикация черновика доступна только администратору. Перед публикацией система проверяет полноту содержимого и, при успехе, рассчитывает контрольную сумму версии.

Проверка при публикации	Условие
Наличие материала	В версии есть хотя бы одна активная тема
Наличие вопросов	Для типа «обучение» — хотя бы один активный вопрос; для типа «ознакомление» вопросы должны отсутствовать
Достаточность банка	Если задано число вопросов в попытке, активных вопросов версии не меньше этого значения
Корректность каждого вопроса	Каждый активный вопрос проходит проверку состава вариантов ответа; при нарушении указывается порядковый номер вопроса и причина
Состояние курса	Курс не находится в архиве

Контрольная сумма версии рассчитывается по алгоритму SHA-256 от канонизированного представления содержимого: заголовков и контрольных сумм текстов тем, минимального времени изучения, перечня вложений с их контрольными суммами, а также вопросов с вариантами ответа и признаками правильности. Идентификаторы записей в расчёт не входят, поэтому две версии с одинаковым содержимым дают одинаковую сумму, а любое изменение материала сумму меняет. Сумма записывается в версию и в неизменяемый журнал вместе с событием публикации.

После публикации версия становится неизменяемой: операции создания, изменения и удаления тем, вложений, вопросов и вариантов ответа допустимы только в контексте черновика. Незавершённые назначения остаются на своей версии — работник дочитывает начатое; новые назначения создаются уже на опубликованной версии.

Архивирование

Курс, утративший актуальность, переводится в архив. Архивирование выполняется мягким удалением: курс снимается с публикации и становится недоступным для новых назначений, но физически не удаляется, поскольку на него ссылаются результаты обучения, сертификаты и записи журнала. Уже пройденное обучение сохраняется и остаётся видимым в истории. Операция идемпотентна: повторный вызов для архивного курса ничего не меняет.

2.3. Темы и вложения

Темы ведутся в контексте черновика версии. Для каждой темы задаются заголовок, форматированное содержимое, признак активности, порядок следования и минимальное время изучения в секундах. Порядок изменяется перетаскиванием; при сохранении порядка система сверяет переданный состав записей с фактическим и отклоняет операцию при расхождении, чтобы одновременная правка двумя сотрудниками не привела к молчаливой перестановке чужих изменений.

Содержимое темы вводится визуальным редактором. Перед сохранением оно очищается на сервере по белому списку тегов и атрибутов. Обработка на стороне браузера защитой не считается и в расчёт не принимается. Встраивание видеозаписей через кадр допускается только с узлов, перечисленных в настройке; пустой перечень означает полный запрет. Изображения, встроенные редактором в виде данных, допускаются для растровых форматов и отбрасываются для векторных.

К теме прикрепляются вложения трёх видов. Тип определяется по фактическому содержимому файла, а не по расширению; проверяются расширение, тип содержимого и размер.

Вид вложения	Допустимые форматы	Предельный размер
Документ	pdf, doc, docx, xls, xlsx, ppt, pptx, odt, txt	100 МБ
Изображение	jpg, jpeg, png, webp	10 МБ
Видеозапись	mp4, webm	500 МБ

Файл сохраняется в приватном объектном хранилище под обезличенным именем; имя, заданное автором, остаётся только в базе данных и не раскрывается в пути объекта. Для каждого вложения рассчитывается и хранится контрольная сумма SHA-256. Вложение может быть помечено как обязательное к просмотру.

2.4. Банк вопросов и параметры проверки знаний

Вопросы ведутся в контексте черновика версии. Экран управления вопросами отображает список с порядком следования, типом, весом и признаком активности; порядок изменяется перетаскиванием с той же сверкой состава, что и для тем.

Тип вопроса	Правила состава	Оценивание
Одиночный выбор	От 2 до 10 вариантов ответа, ровно один правильный	Полный вес при совпадении выбранного варианта с правильным
Множественный выбор	От 2 до 10 вариантов ответа, не менее одного правильного и не менее одного неправильного	Полный вес только при точном совпадении набора выбранных вариантов с набором правильных

Требование наличия хотя бы одного неправильного варианта во множественном выборе введено намеренно: вопрос, все варианты которого правильны, не обладает различающей способностью и не позволяет отличить знание от его отсутствия.

Каждому вопросу задаются вес, учитываемый при подсчёте результата, и необязательное пояснение, показываемое в разборе после завершения попытки.

Параметры проверки знаний задаются на уровне курса, а не версии, и действуют на все циклы обучения по нему.

Параметр	Смысл
Проходной балл	Доля набранного веса в процентах, начиная с которой попытка считается успешной
Число попыток	Предельное число завершённых попыток в пределах цикла. Пустое значение — без ограничения
Пауза между попытками	Минимальный интервал в часах между завершением одной попытки и началом следующей
Ограничение времени	Продолжительность попытки в минутах. Источником истины является серверная отметка времени истечения
Число вопросов в попытке	Размер случайной выборки из банка вопросов версии. Пустое значение — используются все активные вопросы
Срок действия результата	Число месяцев, в течение которых результат считается действующим
Периодичность	Число месяцев, через которое обучение назначается повторно. Пустое значение — разовое обучение

Для курса типа «ознакомление» параметры проходного балла, числа попыток, ограничения времени и числа вопросов в попытке не применяются.

2.5. Назначение обучения вручную и по правилам

Назначение вручную

Экран назначения позволяет выбрать курс и адресатов. Адресаты указываются перечислением работников либо целиком по подразделению, должности или роли. Перед выполнением операции отображается предварительный расчёт: сколько работников попадёт в выборку и скольким из них курс уже назначен в текущем цикле. Задаются срок прохождения и признак обязательности.

Массовое назначение выполняется одной операцией и возвращает сводку: сколько назначений создано, сколько пропущено как уже существующие. Назначение отклоняется, если курс находится в архиве, снят с публикации, не имеет опубликованной версии либо адресат отмечен как уволенный.

Отдельно поддерживается внеочередное назначение — вне графика, по решению ответственного лица, в том числе после компьютерного инцидента. Такое назначение требует указания причины; без причины операция отклоняется. Причина сохраняется в

назначении и фиксируется в неизменяемом журнале.

Правила назначения

Правило описывает, кому и какой курс назначается автоматически. Целью правила выступает подразделение, должность или роль. Правило задаёт курс, признак обязательности и число дней на прохождение, от которого рассчитывается срок.

Правила применяются ежесуточно фоновой задачей, а также запускаются вручную администратором. Применение идемпотентно: работник, которому курс уже назначен в текущем цикле, повторного назначения не получает. Правило может быть временно отключено без удаления. Дублирование правил — вторая запись с той же парой «цель — курс» — отклоняется.

Каждое назначение хранит своё происхождение: создано вручную или правилом, и каким именно правилом. Происхождение наследуется новыми циклами переаттестации, благодаря чему автоматически назначенное обучение продолжает возобновляться автоматически.

Отзыв назначения

Назначение может быть отозвано администратором. Отзыв не удаляет историю: сведения о ранее завершённых циклах и выданных сертификатах сохраняются.

2.6. Циклы переаттестации и сроки

Обучение носит периодический характер. Результат имеет срок действия, по истечении которого работнику назначается новый цикл прохождения. Обработка сроков выполняется ежесуточно фоновыми задачами, порядок запуска которых определён и существенен: сначала создаются назначения, затем меняются статусы, иначе назначение, созданное правилом в текущую ночь, могло бы в тот же прогон оказаться признано просроченным по унаследованному сроку.

Время	Задача	Действие
03:00	Применение правил назначения	Создание назначений работникам, попавшим под действующие правила
03:20	Открытие циклов переаттестации	Создание следующего цикла по результатам, срок действия которых истекает
03:40	Обработка просроченных	Перевод незавершённых назначений с наступившим сроком в состояние «просрочено», отправка эскалации
04:00	Истечение результатов	Перевод пройденных назначений с наступившим сроком действия в состояние «истёк»

04:20	Довыпуск сертификатов	Формирование печатных форм сертификатов, не сформированных при завершении проверки знаний
05:00	Проверка целостности журнала	Пересчёт хеш-цепочки неизменяемого журнала, уведомление администраторов при расхождении
08:00	Напоминания о сроках	Рассылка напоминаний обучаемым. Выполняется в рабочие дни утром, а не ночью
Еженедельно	Обезличивание данных уволенных	Обезличивание персональных данных работников, уволенных ранее установленного срока хранения

Новый цикл создаётся заблаговременно — за настраиваемое число дней до истечения действующего результата, по умолчанию за 30 дней, — чтобы работник успел пройти обучение до того, как его результат перестанет действовать. Операция идемпотентна: назначение, по которому следующий цикл уже создан, в выборку не попадает. Новый цикл всегда создаётся на текущей опубликованной версии и наследует происхождение предыдущего назначения. Циклы не создаются по курсам, снятым с публикации или не имеющим опубликованной версии, а также уволенным работникам.

Обработка сроков выполняется пакетами по 500 записей в транзакции: на организации в несколько тысяч работников поштучное сохранение записей на ежесуточной задаче недопустимо.

2.7. Изучение материалов и подтверждение ознакомления

Обучаемый видит перечень назначенных ему курсов карточками с указанием состояния, срока прохождения, признака обязательности и доли изученных тем. Предусмотрены фильтры по состоянию и поиск.

Экран прохождения разделён на список тем и содержимое выбранной темы. Порядок прохождения линейный: доступ к следующей теме открывается после подтверждения предыдущей. Прямое обращение к теме, до которой обучаемый не дошёл, отклоняется.

Для темы может быть задано минимальное время изучения. Время накапливается по фактическому присутствию на странице темы периодическими отметками, а не вычитанием момента открытия из текущего времени: отметка об открытии проставляется один раз и не сбрасывается, поэтому работник, открывший тему и вернувшийся к ней через час, проходил бы любое минимальное время, ни разу не посмотрев материал. Перед сравнением накопленного времени с минимальным начисляется время, прошедшее с последней отметки, — иначе материал с коротким минимальным временем нельзя было бы подтвердить до следующей отметки, и работник видел бы активную кнопку и отказ сервера в ответ на нажатие.

Подтверждение ознакомления фиксирует реквизиты, по которым спустя годы восстанавливается, с чем именно ознакомился работник:

Реквизит	Назначение
Момент подтверждения	Дата и время фиксации факта
Сетевой адрес	Адрес, с которого выполнено подтверждение
Признак программы просмотра	Строка, переданная браузером работника
Накопленное время изучения	Число секунд фактического присутствия на странице темы
Контрольная сумма содержимого	SHA-256 текста темы на момент подтверждения. Позволяет доказать, что предъявленный материал соответствует изученному
Текст формулировки согласия	Точная формулировка, показанная работнику. Хранится в самой записи, а не берётся из настроек при предъявлении

Операция идемпотентна: повторное подтверждение не изменяет ранее записанные реквизиты. Первое подтверждение в назначении переводит его из состояния «назначено» в состояние «в процессе». Событие записывается в неизменяемый журнал.

Подтверждения относятся к конкретному циклу обучения. Подтверждения предыдущих циклов при переаттестации не засчитываются: повторное обучение требует повторного ознакомления с материалом.

Для курса типа «ознакомление» подтверждение последней активной темы версии переводит назначение в состояние «пройдено» — проверка знаний по такому курсу не предусмотрена.

2.8. Тестирование

Допуск

Перед началом попытки система последовательно проверяет условия допуска и при первом нарушении возвращает причину вместе с готовой формулировкой для интерфейса.

Условие	Сообщение при нарушении
Тип курса	Программа завершается подтверждением ознакомления, проверка знаний не предусмотрена
Доступность курса	Программа временно недоступна
Наличие назначения	Программа не назначена
Состояние назначения	Формулировка зависит от состояния: уже пройдено, попытки исчерпаны, срок действия результата истёк

Изучение материалов	Перед проверкой знаний следует изучить и подтвердить все материалы
Готовность банка вопросов	Проверка знаний пока не подготовлена
Остаток попыток	Все попытки использованы, дальнейшее обучение назначает администратор
Пауза между попытками	Указывается дата и время, начиная с которого доступна следующая попытка

Незавершённая попытка с неистёкшим временем имеет приоритет над всеми ограничениями: работник продолжает начатое, а не начинает заново.

Проведение попытки

Состав попытки — перечень вопросов и порядок вариантов ответа — формируется на сервере при её создании и в дальнейшем не меняется. Ответ на вопрос, не входящий в состав попытки, отклоняется. Состав хранится на сервере; в состоянии страницы не передаются ни полные тексты материалов, ни признаки правильности вариантов.

Экран проверки знаний отображает вопрос, варианты ответа, мини-карту вопросов с признаком отвеченных и обратный отсчёт. Ответы сохраняются по мере выбора; переход между вопросами произволен. Источником истины по времени является серверная отметка истечения: ответы, поступившие после её наступления, не принимаются, а сама попытка завершается автоматически. Одновременно у работника может существовать не более одной незавершённой попытки по курсу.

Результат

Результат рассчитывается как отношение набранного веса к суммарному весу вопросов попытки, выраженное в процентах, и сравнивается с проходным баллом. Отсутствие ответа допустимо и считается неправильным ответом. Для вопросов множественного выбора применяется оценка «всё или ничего».

Экран результата показывает балл, признак прохождения, затраченное время и разбор: по каждому вопросу отображаются выбранные и правильные варианты, признак правильности и пояснение, если оно задано. Успешная попытка переводит назначение в состояние «пройдено», рассчитывает срок действия результата и инициирует выдачу сертификата. Исчерпание попыток переводит назначение в состояние «не пройдено»; дальнейшее прохождение возможно только после назначения нового цикла администратором.

2.9. Сертификаты и протоколы проверки знаний

Выдача сертификата

Сертификат выдаётся автоматически по успешно завершённой попытке. Регистрационный номер сквозной в пределах календарного года и имеет вид «год — порядковый номер из шести цифр». Номер присваивается под блокировкой, чтобы два одновременных завершения проверки знаний не получили один номер; уникальный индекс в базе данных служит второй линией защиты, при коллизии номер пересчитывается.

Срок действия сертификата берётся из назначения цикла, а при его отсутствии рассчитывается по сроку действия результата, заданному в курсе. Каждому сертификату присваивается случайный токен проверки подлинности.

В пределах одного цикла обучения сертификат один: повторный вызов возвращает уже выданный документ. Если печатная форма при этом не сформировалась, повторный вызов инициирует её формирование заново.

Печатная форма формируется фоновой задачей и не задерживает ответ работнику. Сбой постановки задачи в очередь не отменяет выдачу: сертификат уже зарегистрирован, номер присвоен, событие записано в журнал, а файл будет сформирован повтором задачи либо ежесуточной страхующей задачей. Иначе успешно сданная проверка знаний завершалась бы для работника сообщением об ошибке.

Проверка подлинности

Сертификат содержит машиночитаемый код, ведущий на общедоступную страницу проверки. Страница доступна без учётной записи и отображает сведения, достаточные для подтверждения подлинности: регистрационный номер, фамилию и инициалы работника, наименование курса, даты выдачи и окончания действия, состояние документа. Полное имя не раскрывается: для сверки с бумажным сертификатом достаточно фамилии с инициалами. Обращения к странице ограничены по частоте.

Отзыв

Администратор отзывает сертификат с указанием причины. Отозванный документ сохраняется, но отображается как недействительный, в том числе на общедоступной странице проверки. Событие отзыва записывается в неизменяемый журнал.

Протоколы проверки знаний

Протокол формируется по совокупности результатов, отобранных фильтрами: курс, период, подразделение. Документ содержит перечень работников с должностями и подразделениями, результатами, датами прохождения и реквизитами версии курса, по которой проводилась проверка. Протокол предназначен для подшивки и предъявления проверяющему.

Протокол — хранимый документ, а не разовая выгрузка в браузер: разовое формирование не позволило бы впоследствии подтвердить подлинность и целостность документа за весь срок хранения. Протоколу присваивается регистрационный номер вида «год — порядковый номер

из шести цифр», сквозной в пределах календарного года и независимый от нумерации сертификатов; номер печатается в протоколе и присваивается под блокировкой. Для файла рассчитывается и хранится контрольная сумма SHA-256.

Повторный запрос протокола по тем же условиям отбора (курс, подразделение, период, признак отбора только подтвердивших знания) отдаёт уже выданный документ без нового номера — при условии, что состав попыток, вошедших в выборку, не изменился. Тождественность состава определяется контрольной суммой перечня попыток; если условия совпадают, а состав изменился, оформляется новый протокол с новым номером — тихая подмена содержимого под прежним номером недопустима.

Подлинность протокола по регистрационному номеру проверяет персонал с правом просмотра результатов обучения — на той же странице, где формируются протоколы: сверяются условия отбора, состав документа и контрольная сумма файла. В отличие от сертификата, отдельной общедоступной страницы проверки у протокола намеренно нет: протокол — документ о группе работников, и его раскрытие по одной лишь ссылке означало бы массовую выдачу персональных данных постороннему лицу, у которого оказался номер документа.

2.10. Отчётность и выгрузки

Экран результатов обучения отображает назначения всех работников с фильтрами по курсу, состоянию, подразделению, должности, периоду и признаку просрочки, поиском по работнику, сортировкой и постраничной навигацией. Детализация по назначению показывает историю: перечень тем с отметками подтверждения и накопленным временем, перечень попыток с баллами и датами, выданные сертификаты, реквизиты версии.

Панель показателей отображает сводные величины — число назначений по состояниям, долю прошедших обучение, число просроченных — и диаграммы: помесячную динамику прохождения и распределение риска по подразделениям. Диаграммы строятся средствами, входящими в поставку, без обращения к внешним службам.

Выгрузка результатов обучения в формате CSV выполняется синхронно: файл формируется потоковой записью прямо в ответ на запрос и скачивается сразу, без ожидания фоновой обработки. Предел объёма для мгновенной выгрузки — 50 000 строк по текущим фильтрам; при превышении платформа отклоняет выгрузку с указанием числа строк в выборке и предлагает сузить фильтры.

Отдельно, в разделе «Мои выгрузки», доступны выгрузки другого рода — не результатов обучения, а служебных перечней: список пользователей и операционный журнал. Эти выгрузки выполняются фоновой задачей с уведомлением о готовности, а не сразу: их объём не ограничен размером ответа веб-сервера. Готовые файлы хранятся в этом разделе и отдаются по проверке прав.

2.11. Имитационные фишинговые рассылки

Модуль реализует форму обучения, при которой работникам направляется учебное письмо, имитирующее фишинговое, а их реакция фиксируется и используется для адресного дообучения.

Шаблоны

Библиотека шаблонов содержит заготовки писем: тему, отправителя, содержимое, канал доставки и уровень сложности. Содержимое поддерживает подстановку сведений о получателе. Шаблоны переиспользуются между кампаниями.

Кампании

Кампания задаёт шаблон, аудиторию и период проведения. Аудитория указывается перечислением работников либо целиком по подразделению или должности; размер аудитории рассчитывается до запуска.

> **Условие запуска кампании**
>
> Запуск кампании невозможен без подтверждения того, что работники заранее проинформированы о проведении имитационных рассылок локальным нормативным актом. Это требование правового характера, а не организационное удобство, поэтому оно реализовано как техническое ограничение: кто и когда подтвердил информирование, фиксируется в кампании и в неизменяемом журнале и впоследствии не изменяется. Запуск и остановка кампании доступны только администратору.

При запуске проверяются заданность и корректность периода, непустая аудитория и то, что кампания не была запущена ранее. Разворачивание аудитории и постановка писем в очередь вынесены в фоновую задачу: аудитория крупной организации разворачивается не мгновенно, а запуск не должен удерживать администратора в ожидании ответа формы.

Фиксация реакции

Событие	Способ фиксации
Доставлено	Успешная передача письма почтовому шлюзу
Открыто	Запрос изображения-отметки из тела письма
Переход по ссылке	Обращение к учебной странице по персональной ссылке из письма
Ввод учётных данных	Отправка формы на учебной странице. Фиксируется только факт события
Сообщено о подозрительном письме	Действие работника, распознавшего рассылку. Считается положительным исходом

> **Введённые на учебной странице значения не сохраняются**
>
> При событии ввода учётных данных в систему передаются только факт события и обстоятельства запроса — сетевой адрес и признак программы просмотра. Введённые работником значения не передаются в доменный слой, не предусмотрены структурой передаваемых данных и не сохраняются ни в базе данных, ни в журналах.

Фиксация событий идемпотентна: повторное событие того же вида по той же паре «кампания — работник» не создаётся, значимым считается первое. Это не оптимизация, а условие достоверности отчёта: почтовые клиенты запрашивают отметку открытия при каждом просмотре письма и при предварительном просмотре, а по ссылке из письма работник может перейти неограниченное число раз. Защита от одновременных запросов обеспечивается уникальным индексом в базе данных, а не только проверкой перед вставкой.

Обучающая страница и дообучение

Переход по ссылке приводит работника на учебную страницу, объясняющую признаки, по которым письмо можно было распознать. Событие перехода или ввода данных влечёт автоматическое назначение корректирующего микрокурса. Повторное назначение исключается: если работник уже переходил по ссылке, последующий ввод данных микрокурс заново не назначает. Работнику, сообщившему о подозрительном письме, отображается страница благодарности.

Отчётность по кампании

Отчёт по кампании отображает сводные показатели — доли открытий, переходов, вводов и сообщений о подозрительном письме — и поимённый перечень получателей с их реакцией. Разграничение внутри экрана раздельное: сводные показатели доступны при праве управления содержимым курсов, поимённый перечень — только при праве просмотра результатов обучения. Отдельный экран показывает динамику по кварталам.

2.12. Уведомления

Уведомления доставляются по трём каналам: электронной почтой, внутри интерфейса через список оповещений и, при включённой настройке, push-сообщением в браузер. Пользователь управляет каналами в своём профиле по категориям уведомлений. Отправка каждого уведомления регистрируется, что исключает повторную отправку одного и того же напоминания.

Уведомление	Адресат	Повод
Назначено обучение	Обучаемый	Создание назначения вручную или правилом

Приближается срок	Обучаемый	Настраиваемые отметки до срока, по умолчанию за 14, 7 и 1 день
Срок прошёл	Обучаемый	Перевод назначения в состояние «просрочено»
Сводка о просроченных	Менеджер обучения подразделения либо администратор	Наличие просроченных назначений сверх порогового числа. Баллы в сводку не включаются
Предстоит переаттестация	Обучаемый	Приближение окончания срока действия результата
Срок действия результата истёк	Обучаемый	Перевод назначения в состояние «истёк»
Проверка знаний пройдена	Обучаемый	Успешное завершение попытки
Проверка знаний не пройдена	Обучаемый	Неуспешное завершение попытки
Внеочередная проверка знаний	Обучаемый	Внеочередное назначение с указанием причины
Обновлена версия материала	Обучаемый	Принудительный перевод незавершённого назначения на новую версию
Нарушена целостность журнала	Администратор	Расхождение при ежесуточной проверке хеш-цепочки
Не сформирована печатная форма сертификата	Администратор	Исчерпание попыток формирования документа

2.13. Журналирование

Ведутся два журнала различного назначения. Они не дублируют друг друга и не заменяют один другой.

Свойство	Операционный журнал	Неизменяемый журнал
Назначение	Разбор инцидентов и восстановление хода событий	Предъявление проверяющему лицу
Состав записей	Изменения объектов учёта: что, кем и когда изменено, прежние и новые значения	Юридически значимые события: подтверждение ознакомления, завершение попытки, публикация версии, выдача и отзыв сертификата, запуск кампании, доступ к персональным данным

Защита от изменения	Штатные средства разграничения доступа	Хеш-цепочка записей и запрет изменения средствами базы данных
Доступ на просмотр	По отдельному праву	Только администратор

Записи неизменяемого журнала связаны хеш-цепочкой: хеш записи рассчитывается по алгоритму SHA-256 от хеша предыдущей записи и содержимого текущей. Удаление или подмена записи в середине цепочки нарушает все последующие хеши, поэтому подделка задним числом обнаруживается пересчётом.

Неизменяемость обеспечивается на двух уровнях. Триггер базы данных запрещает изменение, удаление и опустошение таблицы, действуя независимо от того, под какой учётной записью подключено приложение, и сохраняясь при восстановлении схемы из резервной копии. Дополнительно при развёртывании рабочей учётной записи приложения выдаются права только на добавление и чтение записей журнала.

Целостность цепочки проверяется ежесуточно фоновой задачей. Расхождение означает вмешательство в обход приложения, поэтому проверка выполняется постоянно, а не только перед предъявлением журнала; при расхождении администраторам направляется уведомление. Проверка выполняется порциями по 1000 записей.

Отдельно фиксируется доступ к персональным данным работников. Открытие списка результатов обучения, просмотр детализации по конкретному работнику и выгрузка результатов записываются в неизменяемый журнал как события доступа. Выгрузка регистрируется до отдачи файла. В журнал записываются идентификаторы субъектов, но не сами персональные данные.

2.14. Справочники, учётные записи, личный кабинет

Справочники подразделений и должностей ведутся администратором и используются при назначении обучения, в правилах назначения и в фильтрах отчётности. Записи справочников удаляются мягко: ссылки на них сохраняются в исторических данных.

Раздел пользователей позволяет вести учётные записи, назначать роли, указывать подразделение, должность и табельный номер, отмечать увольнение. Предусмотрен массовый импорт пользователей из файла. Отметка об увольнении закрывает доступ работника к системе и исключает его из новых назначений и отчётности по просроченным.

Личный кабинет включает редактирование профиля, смену пароля, управление подписками на push-сообщения и настройку каналов уведомлений по категориям. Панель показателей обучаемого отображает назначенные курсы, ближайшие сроки, долю выполнения и дату следующей переаттестации.

3. Роли и разграничение доступа

3.1. Роли

Разграничение доступа построено на ролевой модели: роли присваиваются пользователю, права присваиваются ролям, проверки выполняются по правам, а не по именам ролей, за исключением специально оговорённых операций.

Роль	Объём полномочий
Администратор	Полный доступ к функциям обучения, включая публикацию версий курсов, ведение справочников, отзыв сертификатов, просмотр неизменяемого журнала, запуск и остановку имитационных кампаний, управление ролями, учётными записями, системными настройками и интеграциями, просмотр операционного журнала
Менеджер обучения	Ведение курсов, материалов и вопросов, назначение обучения, просмотр результатов, ведение учётных записей работников, просмотр операционного журнала. Не может публиковать версии, вести справочники подразделений и должностей, просматривать неизменяемый журнал, управлять ролями и системными настройками, запускать и останавливать имитационные кампании
Обучаемый	Прохождение назначенного обучения, просмотр собственного прогресса, результатов и сертификатов

Отдельная роль руководителя подразделения не выделяется. Эскалация просроченных назначений направляется пользователям с ролью менеджера обучения, у которых в профиле указано то же подразделение, а при их отсутствии — администраторам.

3.2. Права доступа

Право	Что открывает	Адм.	Мен.	Обуч.
Просмотр курсов	Пользовательская часть: назначенные курсы, темы, проверка знаний	да	да	да
Управление курсами	Административные экраны курсов, версий, тем, вложений, вопросов, параметров проверки знаний, шаблонов и кампаний имитационных рассылок	да	да	нет
Назначение обучения	Экраны назначения и правил назначения	да	да	нет

Просмотр результатов	Результаты всех работников, детализация, сертификаты, протоколы, поимённые отчёты по кампаниям	да	да	нет
Просмотр собственных результатов	Личный прогресс и собственные сертификаты	да	да	да
Просмотр списка сотрудников	Раздел учётных записей: перечень, карточка, фильтры	да	да	нет
Создание и изменение сотрудников	Заведение учётных записей, назначение роли, подразделения и должности, отметка увольнения, массовый импорт	да	да	нет
Просмотр операционного журнала	Журнал изменений объектов учёта — раздел «Журнал действий», отдельно от неизменяемого журнала	да	да	нет
Управление ролями и правами	Состав ролей и матрица прав	да	нет	нет
Изменение настроек платформы	Системные параметры платформы	да	нет	нет
Настройка интеграций	Параметры внешних интеграций	да	нет	нет

Право просмотра операционного журнала не следует путать с доступом к неизменяемому журналу юридически значимых событий (раздел 2.13): операционный журнал доступен по перечисленному выше праву, неизменяемый — исключительно роли администратора.

Ряд операций ограничен ролью администратора сверх перечисленных прав: публикация версии курса, ведение справочников подразделений и должностей, просмотр неизменяемого журнала, отзыв сертификата, запуск и остановка имитационной кампании, ручной запуск пересчёта правил назначения.

3.3. Уровни проверки прав

Права проверяются на нескольких независимых уровнях. Пропуск любого уровня считается дефектом: уровни закрывают разные способы обращения к функции, и ни один из них не является достаточным сам по себе.

Уровень	Что проверяет	Какое обращение закрывает
Маршрут	Промежуточный обработчик с требованием права или роли	Прямой переход по адресу страницы

Инициализация компонента	Право на экран и принадлежность запрошенного объекта пользователю	Обращение к чужому объекту по его идентификатору при наличии общего права
Метод компонента	Роль или право непосредственно в методе, изменяющем данные	Вызов действия из уже открытой страницы после изменения полномочий
Разметка	Условное отображение элементов управления	Отображение недоступных действий. Самостоятельной защитой не является
Доменный слой	Полномочия, неотделимые от бизнес-правила	Вызов операции в обход интерфейса, например из консольной команды

Почему проверки в методах компонентов обязательны

Компоненты интерфейса вызывают свои публичные методы отдельными запросами к служебной конечной точке, и код инициализации при этом повторно не выполняется. Промежуточные обработчики применяются к таким запросам не в полном составе: применяется проверка подлинности и проверка права, но не проверка роли. Для экрана, закрытого только требованием роли администратора, это означает, что после первой загрузки страницы ограничение перестало бы действовать: снимок состояния компонента остаётся действительным, а роль повторно не сверяется. Работник, у которого роль администратора отозвана, продолжал бы править справочник из уже открытой вкладки.

Поэтому каждый метод, изменяющий данные на экранах, закрытых ролью, сверяет роль самостоятельно — независимо от того, скрыта ли кнопка в разметке и что проверил маршрут. Это реализовано общим примесным типом, подключаемым к таким компонентам.

Аналогичное соображение действует для доменного слоя. Публикация версии курса проверяет роль публикующего внутри самого действия, а не только на экране: действие вызывается в том числе вне пользовательского интерфейса, и ограничение, вынесенное исключительно в интерфейс, при таком вызове не сработало бы.

3.4. Разграничение на уровне данных

Помимо проверки прав применяется разграничение по принадлежности данных. Обучаемый видит только курсы, назначенные лично ему; доступ к темам, вложениям и проверке знаний возможен только через действующее назначение. Прямое обращение по идентификатору без назначения отклоняется. Собственные результаты доступны по праву просмотра собственных результатов, чужие — только по праву просмотра всех результатов.

Вложения и печатные формы сертификатов не отдаются напрямую из хранилища. Отдача выполняется контроллером после проверки прав; для сертификата разграничение выполняет именно контроллер, поскольку правом скачивания обладают и владелец документа, и сотрудник обучающего центра, и выразить это одним требованием на маршруте нельзя.

4. Сквозные процессы

4.1. Жизненный цикл курса

Состояния

Состояние	Признак в данных	Что возможно
Создана	Опубликованная версия отсутствует	Наполнение содержимым. Назначение невозможно
Опубликована	Задана действующая версия, признак активности установлен	Назначение работникам, прохождение обучения
Снята с публикации	Признак активности снят	Действующие назначения продолжаются, новые не создаются
В архиве	Установлена отметка мягкого удаления	Только просмотр истории. Публикация версий и назначения невозможны

Состояния версии

Состояние	Свойства
Черновик	Содержимое изменяется. Работникам недоступна. Одновременно допустим один черновик на курс
Опубликована	Содержимое неизменяемо, рассчитана контрольная сумма, зафиксированы момент публикации и опубликовавший
Действующая	Опубликованная версия, указанная в курсе как текущая. Используется для новых назначений
Историческая	Ранее опубликованная версия. Сохраняется бессрочно: на неё ссылаются завершённые результаты

Переходы

Переход	Инициатор	Условия и последствия
Создание курса	Администратор, менеджер обучения	Задаются наименование, тип, параметры проверки знаний, периодичность и срок действия результата

Создание черновика	Администратор, менеджер обучения	Черновик получает копию содержимого действующей версии. Отклоняется, если черновик уже существует или курс в архиве
Наполнение черновика	Администратор, менеджер обучения	Ведение тем, вложений, вопросов и вариантов ответа
Публикация версии	Только администратор	Проверка полноты содержимого, расчёт контрольной суммы, назначение версии действующей, запись в неизменяемый журнал
Отказ от черновика	Администратор, менеджер обучения	Неопубликованный черновик со своим содержимым удаляется. Опубликованные версии не затрагиваются
Снятие с публикации	Администратор, менеджер обучения	Новые назначения прекращаются, действующие продолжаются
Архивирование	Администратор	Признак активности снимается, курс помечается удалённым мягко. Физического удаления не происходит

4.2. Жизненный цикл назначения обучения

Состояния

Состояние	Смысл	Доступные действия обучаемого
Назначено	Обучение выдано, ни одна тема не подтверждена	Изучение материалов
В процессе	Подтверждена хотя бы одна тема	Изучение материалов, при выполнении условий — проверка знаний
Пройдено	Проверка знаний пройдена либо для типа «ознакомление» подтверждены все темы	Просмотр результата и сертификата
Не пройдено	Попытки исчерпаны без достижения проходного балла	Просмотр результата. Продолжение возможно только после назначения нового цикла

Просрочено	Срок прохождения наступил, обучение не завершено	Изучение материалов и проверка знаний остаются доступны
Истёк	Срок действия ранее полученного результата закончился	Просмотр истории. Обучение возобновляется новым циклом

Переходы

Из состояния	В состояние	Событие перехода
Назначено	В процессе	Первое подтверждение ознакомления с темой
Назначено, В процессе	Просрочено	Ежесуточная задача: наступил срок прохождения, обучение не завершено, работник не уволен
В процессе, Просрочено	Пройдено	Успешно завершённая попытка проверки знаний. Для типа «ознакомление» — подтверждение последней активной темы версии
В процессе, Просрочено	Не пройдено	Завершена последняя доступная попытка, проходной балл не достигнут
Пройдено	Истёк	Ежесуточная задача: наступила дата окончания действия результата
Пройдено	Новый цикл в состоянии «Назначено»	Ежесуточная задача: до окончания действия результата осталось меньше настроенного числа дней. Прежнее назначение сохраняется без изменений

Правила, определяющие поведение циклов

- Назначение всегда относится к одному циклу; номер цикла уникален в пределах пары «работник — курс».
- Прогресс изучения тем, попытки и сертификаты привязаны к циклу. Данные предыдущих циклов не изменяются и остаются доступны в истории.
- Версия курса фиксируется в назначении и не меняется при публикации новой версии: работник завершает начатый цикл на той версии, на которой начал.
- Новый цикл всегда создаётся на текущей опубликованной версии.
- Администратор может принудительно перевести незавершённое назначение на новую версию. Действие требует подтверждения, сбрасывает подтверждения тем текущего цикла и фиксируется в неизменяемом журнале.

4.3. Изучение материалов и подтверждение ознакомления

Шаг	Действие	Результат и проверки
1	Обучаемый открывает курс	Проверяется наличие действующего назначения. Отображается список тем версии, зафиксированной в назначении, с отметками подтверждения текущего цикла
2	Открывает очередную тему	Проверяется доступность: тема либо уже подтверждена, либо является первой неподтверждённой. Фиксируется момент открытия, если он ещё не зафиксирован
3	Изучает материал	Время присутствия на странице накапливается периодическими отметками. Доступны вложения темы
4	Нажимает подтверждение ознакомления	Начисляется время с последней отметки и сверяется с минимальным. При недостатке времени операция отклоняется с указанием, сколько осталось
5	Подтверждение сохраняется	Записываются момент, сетевой адрес, признак программы просмотра, накопленное время, контрольная сумма содержимого и текст формулировки согласия. Событие попадает в неизменяемый журнал
6	Система обновляет состояние	Назначение переводится из «назначено» в «в процессе» при первом подтверждении. Для типа «ознакомление» подтверждение последней темы переводит назначение в «пройдено». Открывается доступ к следующей теме

4.4. Проверка знаний и выдача сертификата

Шаг	Действие	Результат и проверки
1	Обучаемый открывает страницу проверки знаний	Последовательно проверяются условия допуска. При нарушении отображается причина и, если применимо, момент, начиная с которого попытка станет доступна
2	Начинает попытку	На сервере формируется состав попытки: выборка вопросов заданного размера и порядок вариантов ответа. Устанавливается отметка времени истечения. Ограничивается частота обращений
3	Отвечает на вопросы	Ответы сохраняются по мере выбора. Ответ на вопрос вне состава попытки отклоняется. Ответы после наступления отметки истечения не принимаются
4	Завершает попытку	Вручную либо автоматически по истечении времени. Подсчитывается отношение набранного веса к суммарному, результат сравнивается с проходным баллом

5	Система фиксирует результат	Попытка закрывается, событие записывается в неизменяемый журнал. При успехе назначение переводится в «пройдено» и рассчитывается срок действия результата. При исчерпании попыток без успеха — в «не пройдено»
6	Выдаётся сертификат	Только при успешной попытке. Присваивается регистрационный номер под блокировкой, создаётся токен проверки, событие записывается в неизменяемый журнал
7	Формируется печатная форма	Выполняется фоновой задачей и не задерживает ответ. Сбой постановки в очередь не отменяет выдачу: файл будет сформирован повтором задачи либо ежесуточной страхующей задачей
8	Обучаемый видит разбор	По каждому вопросу отображаются выбранные и правильные варианты, признак правильности и пояснение

4.5. Кампания имитационной рассылки

Состояния кампании

Состояние	Смысл
Черновик	Кампания создана, шаблон и аудитория настраиваются, рассылка не начата
Запланирована	Заданы шаблон, аудитория и период проведения, начало отнесено на будущее
Проводится	Письма разосланы или рассылаются, события реакции принимаются и фиксируются
Остановлена	Прервана администратором досрочно. Новые события не принимаются
Завершена	Период проведения окончен. Новые события не принимаются, отчёт доступен

Переходы

Шаг	Действие	Результат и проверки
1	Создание кампании	Указываются наименование, шаблон письма, аудитория и период проведения. Состояние — черновик
2	Расчёт аудитории	Цели разворачиваются в перечень получателей. Отображается размер аудитории

3	Запуск кампании	Доступен только администратору. Обязательно подтверждение информирования работников. Проверяются заданность и корректность периода, непустая аудитория, отсутствие предыдущего запуска. Состояние — «проводится», событие записывается в неизменяемый журнал
4	Рассылка	Выполняется фоновой задачей. Каждому получателю формируется персональная ссылка. Фиксируется событие доставки
5	Реакция работника	Фиксируются открытие, переход по ссылке, отправка формы, сообщение о подозрительном письме. Каждый вид события по паре «кампания — работник» фиксируется однократно
6	Дообучение	Переход по ссылке или отправка формы влекут назначение корректирующего микрокурса. Повторное назначение исключено
7	Завершение	По окончании периода либо по остановке администратором. События больше не принимаются, отчёт по кампании доступен

5. Архитектура

5.1. Слои приложения

Приложение построено по принципу разделения ответственности между тонким слоем интерфейса, доменным слоем и слоем хранения. Разделение не является формальным: каждый слой имеет ограничения, соблюдение которых проверяется при рецензировании и автоматическими проверками.

Слой	Содержимое	Ограничения
Интерфейс	Компоненты страниц, шаблоны разметки, контроллеры отдачи файлов	Проверка ввода, вызов доменного действия, переход и сообщение пользователю. Бизнес-правила здесь не размещаются
Домен	Действия, запросы, объекты передачи данных, перечисления, доменные исключения, службы	Не обращается к текущему запросу, не знает о разметке и маршрутах. Всё необходимое передаётся параметрами
Хранение	Модели предметной области, миграции схемы, фабрики данных	Модели плоские: связи, приведение типов, области выборки. Бизнес-правила в моделях не размещаются
Фоновая обработка	Задания очередей, планировщик, консольные команды	Задание не содержит логики: оно вызывает доменное действие и обрабатывает исход

Доменный слой разбит на ограниченные контексты. Основной контекст — обучение; отдельными контекстами вынесены имитационные рассылки, аутентификация, уведомления, выгрузки, push-сообщения, формирование печатных документов и интеграции.

Связь между контекстами через договорённости

Контекст имитационных рассылок не обращается к контексту обучения напрямую. Он объявляет два интерфейса — регистратор событий в неизменяемом журнале и назначающий внеочередное обучение — и пользуется ими. Реализации, связывающие эти интерфейсы с контекстом обучения, подключаются поставщиком служб. Благодаря этому модуль имитационных рассылок можно исключить из поставки или заменить, не затрагивая учебную часть.

5.2. Размещение бизнес-логики

Бизнес-логика размещается в действиях доменного слоя. Действие имеет один публичный метод, получает зависимости через конструктор и не обращается к текущему запросу: сведения об обстоятельствах — сетевой адрес, признак программы просмотра, инициатор — передаются параметрами. Это делает действие вызываемым одинаково из интерфейса, консольной команды и фоновой задачи.

Сложные выборки вынесены в отдельные объекты запросов, а не размещены в компонентах: списки результатов с фильтрами, сводные показатели, аудитория назначений, данные диаграмм. Компонент получает готовый результат и занимается только его отображением. Отложенная загрузка связей в тестовой среде запрещена: её срабатывание считается ошибкой сборки, что исключает появление запросов в цикле.

Нарушения бизнес-правил выражаются доменными исключениями с осмысленными именами — например, «версия неизменяема», «черновик уже существует», «минимальное время изучения не достигнуто», «требуется причина внеочередного назначения». Слой интерфейса перехватывает их и показывает пользователю пояснение.

5.3. Фоновые задачи и очереди

Продолжительные и отложенные операции выполняются в очередях, обслуживаемых менеджером процессов обработки. В очередь вынесены: формирование печатных форм сертификатов, применение правил назначения, обработка сроков и истечений, выгрузки в формате CSV, рассылка уведомлений, разворачивание аудитории и рассылка имитационных писем, доставка push-сообщений.

Задачи распределены по отдельным группам очередей, чтобы массовая рассылка не задерживала выдачу сертификатов. Периодические задачи объявлены выполняемыми на одном узле и без наложения: при нескольких экземплярах планировщика задача выполняется единожды. Дополнительно задачи объявлены уникальными, что исключает параллельный запуск одной и той же задачи.

Массовые операции выполняются пакетами по 500 записей в транзакции с возможностью продолжения после сбоя. Расписание периодических задач приведено в разделе 2.6.

5.4. Хранение файлов

Файлы размещаются в объектном хранилище, совместимом с протоколом S3, развёрнутом в контуре эксплуатирующей организации. Приватность хранилища обязательна: прямой публичный доступ к содержимому запрещён.

Категория файлов	Порядок хранения и отдачи
Вложения к темам	Обезличенное имя объекта, исходное имя в базе данных, контрольная сумма SHA-256. Отдача контроллером после проверки назначения

Печатные формы сертификатов	Формируются фоновой задачей, хранятся с контрольной суммой. Отдача контроллером с раздельной проверкой прав владельца и сотрудника обучающего центра
Выгрузка результатов обучения (CSV)	Формируется потоковой записью синхронно в ответ на запрос, до 50 000 строк по фильтрам; на диске не хранится
Выгрузки CSV раздела «Мои выгрузки»	Пользователей и операционного журнала. Формируются фоновой задачей, хранятся до скачивания, отдаются по проверке прав
Изображения профиля	Отдаются контроллером под проверкой подлинности

При создании черновика версии файлы вложений не копируются: записи черновика ссылаются на те же объекты хранилища. Содержимое файла неизменно, поэтому дублирование объектов увеличивало бы объём хранилища кратно числу версий, не давая ничего взамен.

5.5. Кэширование

Кэшируются данные, вычисление которых обходится дорого, а изменение происходит редко: состав опубликованных версий курсов, агрегаты прогресса по назначению, счётчики панели показателей, справочные данные. Хранилищем кэша служит сервер структур данных в памяти.

Состав опубликованной версии кэшируется без ограничения по событиям изменения, поскольку опубликованная версия неизменяема по построению. Агрегаты прогресса кэшируются с ключом, включающим работника, курс и цикл, и сбрасываются событиями подтверждения темы, завершения попытки, изменения назначения и публикации версии. Отчётные экраны административной части работают с актуальными данными без кэширования агрегатов: отчёт, показывающий устаревшие сведения, хуже отчёта, который строится дольше.

6. Модель данных

6.1. Сущности и их назначение

Сущность	Чем является
Пользователь	Учётная запись работника. Содержит имя, адрес электронной почты, табельный номер, ссылки на подразделение и должность, отметку об увольнении и отметку об обезличивании
Подразделение, Должность	Справочники организационной структуры. Используются для группировки работников, в правилах назначения и в фильтрах отчётности
Курс	Единица обучения. Содержит наименование, описание, тип, параметры проверки знаний, периодичность, срок действия результата, признак активности и ссылку на действующую версию. Содержимого не содержит
Версия курса	Снимок содержимого. Содержит номер, признак черновика, момент публикации, опубликовавшего и контрольную сумму содержимого
Тема	Раздел учебного материала внутри версии: заголовок, форматированное содержимое, порядок, признак активности, минимальное время изучения
Вложение темы	Файл, прикреплённый к теме: вид, путь объекта в хранилище, исходное имя, тип содержимого, размер, контрольная сумма, признак обязательности просмотра
Вопрос, Вариант ответа	Проверочное задание внутри версии и его варианты. Вопрос содержит тип, формулировку, пояснение, вес и порядок; вариант — текст, признак правильности и порядок
Правило назначения	Описание автоматического назначения: цель, курс, признак обязательности, число дней на прохождение, признак активности
Назначение	Центральная сущность учёта. Связывает работника, курс, зафиксированную версию и номер цикла. Содержит состояние, срок прохождения, дату окончания действия результата, происхождение, ссылку на правило, признак обязательности, причину внеочередного назначения
Прогресс по теме	Факт изучения темы работником в конкретном цикле: моменты открытия и подтверждения, накопленное время, сетевой адрес, признак программы просмотра, контрольная сумма содержимого, текст формулировки согласия

Попытка	Сеанс проверки знаний: работник, курс, версия, цикл, моменты начала, истечения и завершения, балл, признак прохождения, сетевой адрес
Состав попытки	Три сущности, фиксирующие вопросы попытки, ответы работника и выбранные варианты. Обеспечивают воспроизводимость результата спустя годы
Сертификат	Документ о прохождении: работник, курс, версия, попытка, регистрационный номер, даты выдачи и окончания действия, токен проверки, путь печатной формы и её контрольная сумма, отметка отзыва
Запись неизменяемого журнала	Юридически значимое событие: инициатор, сетевой адрес, код события, объект, снимок значимых полей, момент, хеш предыдущей записи и собственный хеш
Шаблон и кампания имитационной рассылки	Заготовка письма и её применение к аудитории в заданный период с фиксацией подтверждения информирования работников
Цель и событие кампании	Получатель рассылки и зафиксированная реакция: вид события, момент, сетевой адрес, признак программы просмотра
Подписка на push-сообщения, Настройка уведомлений	Параметры доставки оповещений конкретному пользователю по каналам и категориям
История паролей, Доверенное устройство, Отложенная проверка входа	Служебные сущности подсистемы аутентификации: запрет повторного использования паролей, запоминание устройства, подтверждение входа кодом
Протокол проверки знаний	Хранимый документ по совокупности результатов: регистрационный номер, условия отбора, состав документа, контрольные суммы содержимого и файла, кто и когда сформировал
Задание выгрузки CSV	Фоновая выгрузка перечня пользователей либо операционного журнала: инициатор, тип, статус, путь к файлу, число строк, отметка завершения

6.2. Связи между сущностями

Связь	Тип	Смысл
Курс — Версия	1 : N	У курса много версий, из которых одна отмечена действующей
Версия — Тема, Версия — Вопрос	1 : N	Содержимое принадлежит версии, а не курсу. Это и делает результат привязанным к материалу

Тема — Вложение	1 : N	Файлы принадлежат теме конкретной версии
Вопрос — Вариант ответа	1 : N	Варианты принадлежат вопросу конкретной версии
Пользователь — Назначение — Курс	N : M	Связь с дополнительными свойствами: цикл, состояние, сроки, версия. Пара «работник — курс» повторяется по числу циклов
Назначение — Версия	N : 1	Версия зафиксирована в назначении и не меняется при публикации новой
Прогресс по теме — Пользователь, Тема, Версия, Цикл	—	Уникальная четвёрка. Подтверждение относится к конкретному циклу и не переносится между циклами
Попытка — Пользователь, Программа, Версия, Цикл	N : 1	Попытка неотделима от цикла: ограничения по числу попыток и паузе считаются в пределах цикла
Попытка — Состав попытки	1 : N	Вопросы, ответы и выбранные варианты сохраняются отдельно от банка вопросов
Сертификат — Попытка	1 : 1	Через попытку сертификат связан с циклом и версией. В пределах цикла действующий сертификат один
Правило назначения — Назначение	1 : N	Назначение помнит породившее его правило; связь наследуется новыми циклами
Кампания — Цель — Событие	1 : N : N	Аудитория и зафиксированная реакция каждого получателя
Запись журнала — Инициатор	N : 1	Связь обнуляемая: журнал переживает удаление учётной записи, имя и адрес на момент события остаются в снимке полей

6.3. Решения, защищающие данные

Неизменяемость журнала юридически значимых событий

Таблица журнала защищена триггером базы данных, отклоняющим изменение, удаление и опустошение. Триггер действует независимо от учётной записи подключения и сохраняется при восстановлении схемы из резервной копии. Рабочей учётной записи приложения при развёртывании выдаются права только на добавление и чтение. Записи связаны хеш-

цепочкой, целостность которой проверяется ежесуточно. Полей времени создания и изменения в таблице нет намеренно: запись неизменяема, а момент события фиксирует отдельное поле.

Запрет физического удаления

Курсы, темы, вопросы и записи справочников удаляются мягко. Причина не в удобстве восстановления, а в том, что на эти записи ссылаются результаты обучения, сертификаты и записи журнала: физическое удаление сделало бы невозможным предъявление сведений о том, чему работник обучался. Архивный курс снимается с публикации и исключается из новых назначений, но остаётся доступным в истории.

Таблицы фактов — назначения, прогресс изучения тем, попытки, состав попыток, сертификаты, события имитационных кампаний — не удаляются вовсе. Их содержимое либо хранится до истечения установленного срока, либо обезличивается.

Привязка результата к версии материала

Содержимое принадлежит версии, а не курсу; версия фиксируется в назначении, в попытке и в сертификате. Опубликованная версия неизменяема, а её контрольная сумма рассчитана по содержимому. Дополнительно контрольная сумма текста темы сохраняется в каждой записи подтверждения ознакомления. Совокупность этих решений позволяет спустя годы показать не только то, что работник прошёл обучение, но и то, каким именно был материал в момент прохождения.

Хранение состава попытки отдельно от банка вопросов

Вопросы попытки, ответы работника и выбранные варианты сохраняются в отдельных таблицах, а не вычисляются заново по банку вопросов при просмотре результата. Правка банка вопросов в новой версии не изменяет ранее полученные результаты и не искажает разбор давно завершённой попытки.

Обезличивание вместо удаления

По истечении срока хранения персональные данные уволенных работников обезличиваются автоматической задачей: сведения, позволяющие определить личность, заменяются, а факты прохождения обучения, результаты и записи журнала сохраняются в обезличенном виде. Учётная запись получает отметку обезличивания. Такой порядок сохраняет отчётность и не удерживает персональные данные дольше установленного срока.

Сохранение результата при отказах смежных подсистем

Регистрация результата не зависит от успешности вспомогательных операций. Сертификат считается выданным в момент присвоения регистрационного номера и записи события в журнал; неудача постановки формирования печатной формы в очередь фиксируется в системном журнале и не отменяет выдачу. Аналогично устроена фиксация подтверждения

ознакомления и завершения попытки.

7. Технические характеристики и требования

7.1. Языки, среды исполнения, библиотеки

Компонент	Технология и версия	Назначение
Язык серверной части	PHP 8.4	Основной язык реализации
Каркас приложения	Laravel 13	Маршрутизация, объектно-реляционное отображение, очереди, планировщик, проверка ввода
Слой интерфейса	Livewire 4, Alpine.js	Серверные компоненты страниц и клиентская интерактивность
Оформление	Bootstrap 5	Сетка, типографика, элементы управления
Сборка ресурсов	Vite, Node.js 22	Сборка стилей и скриптов. При эксплуатации продукта не используется
База данных	PostgreSQL 17	Хранение данных. Используются типы и возможности, специфичные для этой системы: двоичное представление JSON, триггеры, регистронезависимый поиск
Кэш и очереди	Redis Open Source 8.10.0, Horizon	Кэширование, блокировки, очереди заданий и наблюдение за ними
Объектное хранилище	Хранилище, совместимое с протоколом S3	Вложения, печатные формы, выгрузки
Аутентификация	Fortify, подтверждение входа кодом из письма	Вход, восстановление пароля, подтверждение адреса
Разграничение доступа	Библиотека ролей и прав	Ролевая модель
Формирование PDF	Серверная библиотека формирования PDF	Сертификаты, протоколы, организационные документы. Внешние службы не используются
Машиночитаемые коды	Библиотека формирования кодов	Код проверки подлинности на сертификате
Очистка содержимого	Библиотека очистки HTML	Обработка материалов, введённых визуальным редактором

Операционный журнал	Библиотека журналирования изменений	Фиксация изменений объектов учёта
Сбор ошибок	Клиентская библиотека, приёмник разворачивается в контуре организации	Диагностика сбоев. Персональные данные в событиях маскируются
Автоматические проверки	Pest, статический анализ, средство единообразия кода, браузерные проверки	Контроль качества. В поставку продукта не входят

Кэш и очереди работают на Redis Open Source — редакции с открытым исходным кодом, используемой на условиях лицензии AGPL-3.0; коммерческая редакция Redis Enterprise не применяется.

Все используемые сторонние компоненты распространяются на условиях свободных (открытых) лицензий, не содержащих ограничений на использование и распространение на территории Российской Федерации и не препятствующих возникновению исключительного права на программное обеспечение в целом. Выплаты в пользу иностранных правообладателей по лицензионным и иным договорам отсутствуют. Компоненты, распространяемые на условиях лицензий с обязательством предоставления возможности замены библиотеки, поставляются в неизменённом виде.

7.2. Требования к серверу

Рабочий контур включает шесть обязательных контейнерных служб — app, nginx, postgres, redis, horizon, scheduler — и одну опциональную: clamav, антивирусную проверку загружаемых файлов, эксплуатирующая организация включает по потребности. SMTP-сервер и S3-совместимое хранилище объектов в состав поставки не входят и подключаются отдельно, как внешние службы. Состав и запуск приведены в инструкции по установке.

Параметр	Минимально	Рекомендуется для эталонного объёма
Процессор	4 вычислительных ядра	8 вычислительных ядер
Оперативная память	8 ГБ	16 ГБ
Дисковое пространство	100 ГБ	Определяется объёмом вложений: расчёт ведётся от среднего объёма материалов на одну версию с запасом на число версий
Операционная система	Дистрибутив GNU/Linux со средой контейнеризации. Прикладной код не содержит зависимостей от конкретного дистрибутива	

Сетевой доступ	Доступ к настроенным SMTP, S3 и мониторингу; при включённой опциональной антивирусной проверке — также получение антивирусных баз. При установке — к источникам пакетов. Для изолированного контура ресурсы размещаются или зеркалируются внутри него
Транспорт	Защищённое соединение обязательно. Незащищённые соединения перенаправляются

7.3. Требования к рабочему месту пользователя

Специальное программное обеспечение на рабочем месте не требуется: работа ведётся через браузер. Поддерживаются актуальные версии браузеров, реализующих современные веб-стандарты, в том числе построенные на распространённых открытых движках. Обязательны включённая обработка сценариев и поддержка файлов сеанса.

Интерфейс пользовательской части спроектирован от мобильного макета и работоспособен на смартфоне, планшете и настольном компьютере. Административная часть оптимизирована для ширины экрана от 1024 пикселей и остаётся работоспособной на планшете; таблицы получают горизонтальную прокрутку с закреплённым первым столбцом.

Целевой ориентир доступности — уровень АА распространённых рекомендаций по доступности веб-содержимого. Формальная сертификация соответствия не проводилась. Реализованы: достижимость всех элементов управления с клавиатуры с видимой отметкой фокуса, удержание фокуса в модальных окнах с закрытием по клавише отмены, клавиатурное управление на экране проверки знаний, объявление оповещений вспомогательным технологиям, передача состояния результата не только цветом, но и текстом, отключение анимаций при соответствующей системной настройке, работоспособность при масштабировании до 200 процентов.

7.4. Показатели производительности

Показатели заданы для эталонного объёма данных: 5000 работников, 200 курсов, 50 000 действующих назначений, до 10 000 назначений по одному курсу, до 100 тем в курсе и банк до 500 вопросов. Значения приведены для 95-го процентиля времени ответа сервера.

Сценарий	Целевой показатель
Панель показателей обучаемого	менее 300 мс
Перечень назначенных курсов	менее 400 мс
Открытие темы в курсе объёмом до 100 тем	менее 400 мс
Начало попытки при банке 500 вопросов	менее 800 мс

Сохранение ответа на вопрос	менее 200 мс
Завершение попытки на 100 вопросов	менее 1,5 с
Перечень результатов с фильтрами при 50 000 назначений	менее 800 мс
Панель показателей администратора	менее 700 мс
Формирование печатной формы сертификата	в очереди, ответ пользователю не задерживается
Выгрузка результатов обучения (CSV, до 50 000 строк)	синхронно, потоковой записью в ответ
Фоновая выгрузка (пользователи, операционный журнал)	в очереди с уведомлением о готовности
Одновременное прохождение проверки знаний	200 работников без ухудшения показателей более чем на 50 процентов

Достижение показателей обеспечивается набором реализационных решений: запретом отложенной загрузки связей, обязательной постраничной навигацией во всех перечнях, загрузкой перечня тем без содержимого, кэшированием агрегатов прогресса, покрывающими индексами под запросы экранов со списками, вынесением продолжительных операций в очереди и пакетной обработкой массовых операций.

Основание приведённых значений

Значения представляют собой проектные целевые показатели, заданные для эталонного объёма данных, и подтверждаются нагрузочным испытанием на наполненной базе. Результаты испытания на инфраструктуре эксплуатирующей организации оформляются отдельным протоколом, поскольку зависят от характеристик конкретной площадки.

8. Безопасность

Разграничение доступа

Применяется ролевая модель с проверками на нескольких независимых уровнях: промежуточный обработчик маршрута, инициализация компонента страницы, метод компонента, изменяющий данные, условное отображение в разметке и доменный слой. Обоснование обязательности проверки в методах компонентов приведено в разделе 3.3. Все маршруты, кроме общедоступной страницы проверки подлинности сертификата и служебных ресурсов веб-приложения, требуют подтверждённого входа.

Парольная политика

Требование	Значение
Минимальная длина	12 символов, настраивается
Состав	Обязательное присутствие символов нескольких категорий: букв разного регистра, цифр, специальных символов
Проверка по перечню скомпрометированных	Предусмотрена и по умолчанию отключена. Проверка выполняется обращением к внешнему источнику сведений об утечках, поэтому в поставке она выключена: платформа рассчитана на работу в контуре организации без обращений к внешним сетям. Включается настройкой, если контур такие обращения допускает
Запрет повторного использования	Проверяется по истории ранее применявшихся паролей
Смена при первом входе	Обязательна. Учётная запись, созданная администратором или загруженная списком, помечается требующей смены пароля: до неё работник не допускается к разделам платформы. Отметка снимается после успешной смены
Максимальный срок действия	Настраивается числом суток. Время последней смены пароля фиксируется; по истечении установленного срока платформа требует сменить пароль тем же порядком, что и при первом входе. По умолчанию ограничение отключено — срок устанавливается локальным нормативным актом эксплуатирующей организации

Подтверждение входа кодом

После проверки пароля вход подтверждается одноразовым кодом, направляемым на адрес электронной почты работника. Код имеет ограниченный срок действия; число попыток ввода ограничено; повторная отправка ограничена по частоте. Устройство может быть отмечено доверенным на ограниченный срок, что избавляет от повторного подтверждения.

Просроченные отложенные проверки и отметки доверенных устройств удаляются ежесуточной задачей. Подтверждение входа кодом применяется единообразно ко всем ролям и не зависит от полномочий работника: по умолчанию мера включена для всех учётных записей сразу, а отключить её может только эксплуатирующая организация настройкой на уровне всей платформы — самостоятельно отключить подтверждение для своей учётной записи работник не может. Для отдельной учётной записи администратор сервера консольной командой может назначить временное освобождение от кода на срок, заданный в днях при выполнении команды, не затрагивающее остальные учётные записи.

Блокировка учётной записи

Неуспешные попытки входа учитываются. По достижении установленного числа попыток за контрольный период учётная запись временно блокируется; работнику направляется уведомление о блокировке. Блокировка снимается по истечении срока либо действием администратора. Ограничение частоты применяется также к подтверждению входа, началу попытки проверки знаний, сохранению ответа, скачиванию файлов и общедоступной проверке сертификата.

Политика безопасности содержимого

Приложение устанавливает на каждый ответ пользовательской части заголовки безопасности: запрет угадывания типа содержимого браузером, ограничение встраивания страницы в кадр, ограничение передачи адреса источника перехода и политику безопасности содержимого.

Политика является действующей, а не наблюдательной: она блокирует выполнение постороннего кода, а не только сообщает о нём. Доверие к собственным встроенным сценариям выражается одноразовым значением, создаваемым заново на каждый запрос и подставляемым только в те теги, которые входят в состав приложения. Внедрённый в страницу посторонний сценарий этого значения не знает и не будет выполнен, даже если разметка окажется уязвимой. Для таблиц стилей, создаваемых веб-компонентом значков уже после отправки заголовка, доверие выражается контрольными суммами конкретных строк, а не общим послаблением: разрешена не встроенная таблица стилей вообще, а ровно известное содержимое. Директивы источников ограничены собственным узлом, что исключает загрузку ресурсов и обращения к посторонним узлам. Нарушения политики принимаются отдельной конечной точкой для разбора.

Санитизация пользовательского содержимого

Форматированное содержимое тем и описаний курсов очищается на сервере по белому списку тегов и атрибутов перед сохранением. Обработка на стороне браузера защитой не считается. Встраивание кадров допускается только с узлов, явно перечисленных в настройке; пустой перечень означает полный запрет. Векторные изображения, встроенные в виде данных, отбрасываются всегда.

Загружаемые файлы проверяются по расширению, фактическому типу содержимого и размеру; тип определяется по содержимому, а не по расширению. Файлы сохраняются в приватном хранилище под обезличенными именами, для каждого рассчитывается контрольная сумма. Отдача выполняется контроллером после проверки прав с заголовками, предписывающими сохранение файла и запрещающими угадывание типа.

Журналирование доступа к персональным данным

Открытие перечня результатов обучения, просмотр детализации по конкретному работнику и выгрузка результатов фиксируются в неизменяемом журнале как события доступа к персональным данным. Выгрузка регистрируется до отдачи файла. В журнал записываются идентификаторы субъектов и состав применённых фильтров, но не сами персональные данные. Записи журнала защищены от изменения и удаления, как описано в разделе 6.3.

Локализация данных

База данных, кэш, очереди, S3-хранилище, почтовый шлюз и приёмник ошибок размещаются в согласованном контуре, включая услуги российского провайдера. Адреса SMTP, S3 и мониторинга задаются конфигурацией; доступ к ним необходим для работы соответствующих функций. Шрифты, скрипты и значки поставляются локально.

Дополнительно могут включаться проверка пароля по перечню утечек и push-уведомления через службы браузеров. Обе функции выключены по умолчанию. В полностью изолированном контуре они остаются выключенными, а SMTP, S3, мониторинг и обновления антивирусных баз обеспечиваются внутренними ресурсами.

Прочие меры

Мера	Реализация
Защита от подделки запросов	Штатный механизм каркаса для всех форм
Защита от массового присвоения	Явное объявление полей, доступных для присвоения, в каждой модели
Защита от внедрения в запросы к базе	Объектно-реляционное отображение и параметризованные запросы
Управление сеансами	Файлы сеанса с признаками защищённой передачи, недоступности сценариям и ограничения передачи между узлами. Завершение всех сеансов при смене пароля
Маскирование в событиях об ошибках	Тела запросов и их параметры не передаются, пользователь обозначается числовым идентификатором
Резервное копирование	Ежесуточное создание копии базы данных с ротацией. Порядок восстановления описан в эксплуатационной документации

Разделение сред	В испытательных и демонстрационных средах применяются синтетические данные

9. Ограничения и известные особенности

9.1. Не входит в область применения

Перечисленное не реализовано в текущей версии. Перечень приведён для того, чтобы очертить границы продукта и исключить неверные ожидания при внедрении.

Функция	Пояснение
Обслуживание нескольких организаций одним экземпляром	Экземпляр обслуживает одну организацию. Разделение по арендаторам не заложено в модель данных. Обслуживание нескольких организаций выполняется установкой отдельных экземпляров
Самостоятельная запись на обучение, открытый каталог	Обучение только назначается администратором либо правилом
Платное обучение, расчёты с обучаемыми	Коммерческие функции не предусмотрены
Учёт очных мероприятий, расписание, аудитории, преподаватели	Не автоматизируется. Результат очного мероприятия вносится как курс типа «ознакомление» либо учитывается вне системы
Вебинары, видеоконференции, обсуждения между обучаемыми	Средства общения не предусмотрены
Игровые механики: баллы, значки, рейтинги	Не предусмотрены
Вопросы на упорядочение, сопоставление и со свободным ответом	Предусмотрены структурой данных, но недоступны для создания. Попытка сохранить такой вопрос отклоняется
Ручная проверка развёрнутых ответов	Следует из предыдущего пункта: оценивание полностью автоматическое
Адаптивные траектории, персональные рекомендации	Порядок прохождения линейный и одинаковый для всех
Контроль условий прохождения проверки знаний по видеоканалу	Не реализовано в текущей версии
Обмен данными с внешними системами обучения по отраслевым форматам	Не предусмотрен
Автоматическая синхронизация с кадровой системой	Справочники подразделений и должностей и учётные записи ведутся вручную либо загружаются файлом

Программный интерфейс для внешних систем	Общедоступный программный интерфейс не предусмотрен
Мобильное приложение	Применяется адаптивная веб-версия
Интерфейс на иных языках	Интерфейс только на русском языке
Усиленная электронная подпись	Подтверждение ознакомления реализовано как простая электронная подпись. Работа с сертификатами ключей проверки не предусмотрена

9.2. Функции, требующие внешних условий

Функция	Требуемое условие
Push-уведомления в браузер	Функция дополнительная и включается настройкой. Требует формирования пары ключей и доступа к сети общего пользования, поскольку стандарт Web Push предусматривает доставку через службы производителей браузеров. При отключении функции оповещения доставляются электронной почтой и отображаются внутри интерфейса; основная функциональность не затрагивается
Рассылка уведомлений и имитационных писем	Требуется настроенный почтовый шлюз. Без него уведомления накапливаются в очереди
Хранение вложений и печатных форм	Требуется развёрнутое объектное хранилище, совместимое с протоколом S3, с закрытым публичным доступом
Периодические задачи	Требуется запущенный планировщик и хотя бы один обработчик очередей. Без них не создаются циклы переаттестации, не меняются состояния по срокам, не формируются печатные формы и не рассылаются напоминания
Полная неизменяемость журнала	Триггер базы данных действует всегда. Дополнительное ограничение прав рабочей учётной записи приложения выполняется при развёртывании, поскольку её имя задаётся параметрами среды
Запуск имитационных кампаний	Требуется предварительное информирование работников локальным нормативным актом. Без подтверждения этого факта запуск технически невозможен
Встраивание видеозаписей по ссылке	Требуется явное указание доверенных узлов в настройке. По умолчанию перечень пуст и встраивание запрещено
Сроки хранения и обезличивания	Значения задаются настройкой и подлежат установлению эксплуатирующей организацией исходя из применимых к ней требований

Периодичность обучения и переаттестации	Конкретные значения устанавливает эксплуатирующая организация локальным нормативным актом. Система обеспечивает исполнение заданных значений, но не определяет их

9.3. Особенности, влияющие на эксплуатацию

Особенность	Что следует учитывать
Опубликованная версия неизменяема	Исправление опечатки в опубликованном материале требует создания черновика и публикации новой версии. Изменить опубликованный материал «на месте» нельзя. Это следствие требования доказуемости, а не недоработка
Один черновик на курс	Параллельная подготовка двух редакций одного курса не поддерживается
Курсы не удаляются	Доступно только архивирование. Перечень архивных курсов со временем растёт и отображается по отдельному фильтру
Подтверждения не переносятся между циклами	При переаттестации работник изучает материал заново, даже если он не изменился
Перевод назначения на новую версию сбрасывает подтверждения	Действие принудительное, требует подтверждения администратором и фиксируется в неизменяемом журнале. Применяется, когда материал изменён существенно
Порядок ночных задач существенен	Изменение времени запуска периодических задач без учёта их взаимной последовательности приводит к неверным состояниям назначений
Значения, введённые на учебной странице имитационной рассылки, не сохраняются	Отчёт по кампании показывает факт ввода, но не содержание. Восстановить введённые значения невозможно, и это сделано намеренно
Расхождение хеш-цепочки журнала	Означает вмешательство в базу данных в обход приложения. Требует разбора, а не повторного расчёта цепочки
Антивирусная проверка загружаемых файлов	Приложение проверяет расширение, тип и размер файла и, если проверка включена (ANTIVIRUS_ENABLED=true и профиль antivirus — опционально, решение эксплуатирующей организации), передаёт файл ClamAV. При включённой проверке недоступность сканера отклоняет загрузку. См. разделы 4.2 и 5.4 инструкции по установке
Обезличивание необратимо	После обезличивания восстановить персональные данные работника невозможно. Отчётность по обезличенным записям сохраняется в обезличенном виде

Организационные документы эксплуатирующей организации

Продукт реализует технические меры и обеспечивает исполнение установленных правил, но не подменяет организационно-распорядительные документы оператора. Модель угроз, акт классификации информационной системы, положение об обработке персональных данных, локальные нормативные акты о периодичности обучения и о проведении имитационных рассылок, сроки хранения и порядок реагирования на инциденты разрабатываются и утверждаются эксплуатирующей организацией. Аттестация информационной системы, если она требуется, выполняется эксплуатирующей организацией с привлечением организации, имеющей соответствующую лицензию.