Приложение 1 к документации о закупке

**Техническое задание**

**на внедрение системы управления корпоративным обучением  
для нужд АО «ЭнергосбыТ Плюс»**

1. **Наименование услуги:** Внедрение системы управления корпоративным обучением (далее – Система).
2. **Место использования:** Использование Программных продуктов допускается на территории Российской Федерации.
3. **Сроки оказания услуги:** 42 месяца с даты подписания Договора.
4. **Общие сведения**

## Термины и сокращения

Специальные термины, используемые в настоящем ТЗ, приведены в таблице ниже.

| **Термин** | **Описание** |
| --- | --- |
| Заказчик | АО «ЭнергосбыТ Плюс» |
| Исполнитель | Исполнитель работ по внедрению Системы |
| Система | Автоматизированная информационная система управления корпоративным обучением |
| БД | База данных |
| ОПЭ | Опытно-промышленная эксплуатация |
| ПО | Программное обеспечение |
| ПСИ | Приемо-сдаточные испытания |
| ТЗ | Техническое задание |

## Назначение документа

Документ формирует цели и задачи АО «ЭнергосбыТ Плюс» (далее – Заказчик), ожидания от реализации Проекта «Система управления корпоративным обучением» (далее – Проект).

Детализация документа является высокоуровневой, включающей потребности Заказчика, краткие характеристики системы и описание технических и функциональных требований.

Контроль услуг осуществляется Заказчиком в соответствии с требованиями Технического задания. Предмет Технического задания

В рамках выполнения услуг по настоящему Техническому заданию Исполнитель должен выполнить поставку системы управления корпоративным обучением (далее – Система), выполнить ее установку на серверах заказчика, выполнить настройку системы в соответствии с требованиями настоящего ТЗ и осуществить гарантийную и техническую поддержку системы.

## Краткое описание Проекта

У Заказчика отсутствует собственная система управления корпоративным обучением. Требуется внедрить новую систему управления корпоративным обучением на базе готового продукта.

Система включает набор программных продуктов и решений, который объединяет и автоматизирует большую часть процессов, связанных с обучением, а именно:

• организация и управление всеми видами обучения (дистанционное и синхронное обучение (в формате вебинаров, онлайн-тренингов, очного обучения), включая сбор заявок, регистрацию, рассылку напоминаний участникам, проведение занятия в системах организации онлайн-обучения с бесшовной интеграцией, аналитика по результатам и посттренинговое обучение);

• сбор потребностей в обучении, управление заявками на внешнее обучение (согласование, администрирование);

* тестирование знаний, навыков, проверка компетенций;

• размещение и предоставление учебного и познавательного контента различных форматов (аудио- и видеофайлы, книги, статьи, тесты, курсы и т.п.) и образовательных программ, в том числе возможность добавления материалов и курсов с внешних платформ;

• встроенный конструктор с вышеперечисленными форматами, а также форматами Tilda, Typeform, PDF, поддержка форматов SCORM 1.2 и 2004 для создания комплексных программ, курсов и тестов.

• хранилище образовательного контента и ведение архива учебных материалов, медиафайлов;

• календарь-планировщик событий, возможность планирования учебных курсов;

• встроенный функционал для проведения вебинаров либо возможность включения в курс активной ссылки на площадку для проведения вебинаров;

• сбор, хранение и обработка результатов оценки и обучения персонала, формирование разного вида отчетностей для анализа всех видов обучения;

• API-интеграция с системами кадрового учета, календарем компании;

• встроенный модуль оценки персонала;

• создание индивидуальных планов обучения;

• личный кабинет администратора, руководителя, пользователя с разными уровнями доступа к аналитике относительно ролей;

• мобильная версия системы с возможностью прохождения обучения оффлайн;

• геймификация/система мотивации и поощрения пользователей за активные действия в системе обучения;

• непрерывное обеспечение доступа к обучению вне зависимости от локации и каналов доступа.

Проект включает возможность Системы поддерживать курсы и обеспечить неограниченное количества доступов пользователей в Систему.

## Организационный объем

Система предполагается к внедрению в компании АО «ЭнергосбыТ Плюс» с возможностью неограниченного добавления пользователей в Систему.

Система должна иметь возможность подключения новых филиалов компании без доработок.

Заказчик должен иметь право тиражирования Системы в иных юридических лицах внутри группы компании ПАО «Т Плюс» без приобретения дополнительных лицензий и заключения договоров.

## Плановые сроки начала и окончания работ

Срок начала работ по настоящему проекту – дата подписания договора.

Срок окончания работ по этапу внедрения и настройке Системы – 6 месяцев после подписания договора.

Срок окончания технической поддержки системы – 4 календарных года с даты окончания работ по внедрению Системы.

Укрупнённый план-график содержится в пункте 5 данного ТЗ.

Результаты работ оформляются и предъявляются Заказчику поэтапно в соответствии в планом-графиком, содержащимся в Договоре между Исполнителем и Заказчиком. Предлагаемый план-график представлен в пункте 5 данного ТЗ.

## Гарантийный срок

Гарантийная поддержка Системы/ПО осуществляется силами Исполнителя в течение 12-и (двенадцати) месяцев с момента внедрения Системы.

1. **Общие и технические требования**

## Требования к структуре и функционированию Системы

Функциональные требования к Системе приведены в Приложении №1 к данному ТЗ «Функциональная спецификация».

## Требования к методическому обеспечению

Функционал Системы и все ее компоненты должны соответствовать требованиям настоящего ТЗ, а также документации, разработанной при оказании услуг, предусмотренных в проекте в соответствии с настоящим ТЗ.

## Требования к интеграции

В рамках предоставления услуг по Проекту Исполнитель должен интегрировать Систему со смежными системами:

• через интеграционную шину с 1С Единая справочная система в части обмена данными по сотрудникам;

• прямая интеграция с Active Directory в части доменной авторизации.

Система должна предусматривать возможность интеграции с дополнительными внешними сервисами по API.

## Требования по диагностированию Системы

Диагностирование Системы должно обеспечивать выявление неработоспособности технических средств, базового и прикладного ПО. Для поддержания установленных параметров качества обслуживания, Система должна обеспечивать протоколирование системных ошибок и действий пользователей с возможностью последующего анализа возникновения критических ситуаций (log-файлы).

Система не должна требовать использования нештатных режимов работы серверов баз данных, серверов приложений и каналов связи для штатного функционирования.

Система должна удовлетворять следующим требованиям по диагностированию:

• запись при возникновении системных ошибок в ходе выполнения работы в системный журнал;

• протоколирование действий пользователей̆ при предоставлении услуги;

• выдача пользователю сообщений, содержащих описание нарушения работоспособности.

## Требования к порядку подготовки персонала, контролю его знаний и навыков

В целях подготовки персонала Заказчика к работе с Системой Исполнитель должен:

• провести консультации для персонала Заказчика по работе с Системой (в формате вебинара(-ов) по особенностям работы каждой из ролей);

• разработать и передать Заказчику инструкции на русском языке по работе с Системой по каждой роли с описанием всего процесса администрирования программного обеспечения, записи вебинаров, доступ к материалам по Системе.

## Показатели назначения

Система должна предусматривать возможность масштабирования по производительности и объему обрабатываемой информации.

## Требования к эргономике и технической эстетике

Визуальный интерфейс системы должен быть современным, понятным и удобным, легким в освоении пользователями, не должен быть перегружен графическими элементами и должен обеспечивать быстрое отображение экранных форм.

Навигационные элементы должны быть выполнены в удобной для пользователя форме. Средства редактирования информации должны удовлетворять принятым соглашениям в части использования функциональных клавиш, режимов работы, поиска, использования оконной системы. Ввод-вывод данных, прием управляющих команд и отображение результатов их исполнения должны выполняться в интерактивном режиме. Интерфейс должен соответствовать современным эргономическим требованиям и обеспечивать удобный доступ к основным функциям и операциям Системы.

Интерфейс должен быть рассчитан на преимущественное использование манипулятора типа «мышь», то есть управление Системой должно осуществляться с помощью набора экранных меню, кнопок, значков и т. п. элементов. Клавиатурный режим ввода должен использоваться главным образом при заполнении и/или редактировании текстовых и числовых полей экранных форм.

Интерфейс Системы должен быть выполнен в едином графическом дизайне с одинаковым расположением основных элементов управления и навигации. Дизайн портала и мобильного приложения должен быть оформлен согласно брэндбуку Заказчика с использованием корпоративных цветов, заменой домена, логотипа.

Должна быть предусмотрена возможность работы с Системой посредством WEB-браузеров (IE, Edge, Google Chrome, Safari, Yandex, Mozilla Firefox после 2020 г. и более поздние), интерфейс должен быть адаптирован для WEB-браузеров мобильных устройств (операционная система iOs 12 или выше, Аndroid 6 или выше).

Взаимодействие пользователей с программным комплексом должно осуществляться посредством визуального графического интерфейса (GUI). В качестве основного средства для реализации визуального графического интерфейса должны использоваться средства веб-интерфейса.

## Требования к защите информации от несанкционированного доступа

Уровень конфиденциальности информации, обрабатываемой в Системе, принадлежит к категории «Конфиденциальная», режим доступа к информации многопользовательский. Информационная система должна обеспечивать защиту от несанкционированного доступа (НСД) на уровне не ниже установленного требованиями, предъявляемыми к категории 1Г по классификации действующего руководящего документа Гостехкомиссии России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» 1992 г.

Уровень защищённости от несанкционированного доступа средств вычислительной техники, обрабатывающих информацию, должен соответствовать требованиям к классу защищённости 5 СВТ согласно требованиям действующего руководящего документа Гостехкомиссии России «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации».

Исполнитель гарантирует, что в рамках данного ТЗ ПО, к которому предоставлен доступ, позволяет выполнить эти требования. Исполнитель не отвечает за стороннее ПО.

Информационная система не требует обязательных государственных аттестационных испытаний по требованиям информационной безопасности.

Защита информации в Системе должна обеспечиваться техническими средствами и поддерживающими их организационными мерами в соответствии с регламентирующими документами организации Заказчика.

Доступ пользователей к функциям и данным Системы должен предоставляться только после прохождения пользователем процедур аутентификации и авторизации.

Доступ пользователей к функциям и данным Системы должен быть ограничен на основе группового и ролевого принципа.

Каждому пользователю Системы должна быть сопоставлена учетная запись, ассоциированная с одной или несколькими предопределенными пользовательскими группами. При назначении нескольких пользовательских групп пользователь должен получать расширенные права в соответствии с объемом доступа назначенных пользовательских групп. Назначение в группу доступа должно позволять управлять доступом пользователя к следующим функциям:

• пунктам меню;

• представлениям реестров;

• аналитическим панелям (дашбордам) на главной странице Системы;

• возможности создания объектов Системы, доступных для создания из реестров.

Необходимо обеспечить обязательное ведение журнала событий в Системе с указанием типовых значений для каждого события в Системе (создание, редактирование).

В журнале событий должны фиксироваться все типовые действия всех пользователей по созданию и редактированию объектов Системы.

Должна быть предусмотрена возможность формирования журнала событий за произвольный период времени.

## Требования к патентной чистоте

В результате создания Системы должна быть предусмотрена передача Заказчику прав использования ПО, поставляемого Исполнителем в рамках оказания услуг, на условиях простой (неисключительной) лицензии.

Установка системы в целом, как и установка отдельных частей системы не должна предъявлять дополнительных требований к покупке лицензий на программное обеспечение сторонних производителей, кроме программного обеспечения, входящего в состав информационной системы и приобретаемого в рамках настоящего Технического Задания.

Патентная чистота Системы и ее частей должна быть обеспечена в отношении патентов, действующих на территории Российской Федерации.

Реализация технических, программных, организационных и иных решений, предусмотренных проектом Системы, не должна приводить к нарушению авторских прав и смежных прав третьих лиц.

В случае если для оказания услуг и достижения установленных Техническим заданием результатов возникает необходимость в использовании иных результатов интеллектуальной деятельности, исключительные права на которые принадлежат третьим лицам, Исполнитель уведомляет об этом Заказчика в письменной форме и по согласованию с Заказчиком заключает лицензионные (сублицензионные) договоры, которые требуются для оказания услуг и достижения установленных Техническим заданием результатов. Исполнитель предоставляет (обеспечивает предоставление) Заказчику прав использования таких результатов интеллектуальной деятельности, исключительные права на которые принадлежат третьим лицам, по соответствующему лицензионному (сублицензионному) договору не позднее даты предоставления Заказчику услуг.

В случае если для оказания услуги установленных Техническим заданием результатов возникает необходимость в использовании результатов интеллектуальной деятельности, которые были ранее созданы (разработаны) Исполнителем и исключительные права на которые принадлежат Исполнителю, Исполнитель уведомляет об этом Заказчика в письменной форме и, по согласованию с Заказчиком предоставляет Заказчику права использования таких результатов интеллектуальной деятельности по соответствующему лицензионному договору не позднее даты окончания предоставления Заказчику услуг.

## Требования к надежности технических средств и программного обеспечения

Отказы и сбои в работе рабочих станций и сетевого оборудования не должны приводить к разрушению данных и сказываться на работоспособности Системы в целом.

Система должна обладать надежностью, обеспечивающей работу пользователей в штатном режиме и оперативное восстановление работоспособности при сбоях.

Действия пользователей не должны приводить к потере информации или «зависанию» ПО.

Должна быть предусмотрена отказоустойчивость на уровне программной платформы.

В Системе должен быть предусмотрен автоматизированный механизм протоколирования осуществляемых операций.

Система должна обеспечивать обнаружение и диагностику ошибок с выдачей соответствующих сообщений администратору через лог-запись. В лог должна попасть информация обо всем пути выполнения операций, которые привели к сбою, без необходимости включать другой уровень логирования и ловить ошибку заново.

Система должна производить уведомление администраторов обо всех фактах сбоев в том числе в интерактивном режиме.

Программные средства должны содержать средства контроля вводимой информации и средства защиты от несанкционированных действий, "спама" и атак с внешних систем, а также средства контроля, резервирования и восстановления данных.

Для этого в Системе должны быть предусмотрены:

• контроль целостности данных на уровне СУБД;

• сохранение целостности данных в базе данных при нештатном завершении программы;

• сохранение работоспособности программного обеспечения при некорректных действиях пользователя;

• автоматическая поддержка данных в непротиворечивом состоянии и стабильная работа Системы при многопользовательском режиме работы;

• средства обеспечения резервного копирования и восстановления данных для всех используемых и обеспечивающих работу инфраструктурных сервисов и приложений.

Аппаратные и программные средства, необходимые для развертывания системы, а также осуществления операций по резервному копированию и восстановлению предоставляются Заказчиком по рекомендуемым Исполнителем характеристикам, приведенным в разделе Требования к программному обеспечению, Требования к аппаратному обеспечению.

## Требования к режимам функционирования Системы

Система должна функционировать в следующих режимах:

• штатный режим;

• сервисный режим.

Штатный режим работы является основным, при котором обеспечивается непрерывная круглосуточная работа аппаратно-программных средств и неограниченный доступ для пользователей Системы.

В сервисном режиме осуществляются все работы по модернизации, проведение планового обслуживания, реконфигурация существующих модулей, а также резервное копирование всей информации.

Диагностирование должно осуществляться путем анализа записей в системных журналах, что обеспечит:

• Выявление сбоев и отказов в работе Системы;

• Выявление нарушений целостности данных;

• Обнаружение состояний, предшествующих возникновению отказов и сбоев, которые подлежат диагностике.

Отсутствие договора на техническую поддержку лицензий/Системы между Заказчиком и вендором приобретаемого ПО не должно ограничивать функциональность поставленного ПО для Заказчика.

## Требования к программному обеспечению

Программное обеспечение Системы должно отвечать следующим требованиям.

Веб-сервер:

* Операционная система CentOS 7, AlmaLinux 8, 9
* Предусмотрено логирование всех принятых запросов и действий веб-сервера.

При наличии Сервера баз данных, он должен отвечать следующим требованиям:

* Операционная система CentOS 7, AlmaLinux 8, 9
* PostgreSQL 9.6, 11, 12.

## Требования к поставке Программного комплекса

* Все компоненты программного комплекса должны иметь документацию, описывающую внутреннее устройство, способы использования, администрирования, развёртывания и полного удаления.
* Система должен иметь механизмы непрерывной интеграции с этапами сборки, тестирования и развёртывания.
* Ядро системы должно быть установлено на оборудовании, предложенном Заказчиком.
* Исполнитель гарантирует, что предоставленное программное обеспечение будет функционировать в полном объеме в соответствии с ТЗ и не потребует заключения дополнительных договоров на различные сервисные функции без которых работа представленного программного обеспечения будет невозможной.
* Система и ее компоненты, включая тестовые, не могут размещаться на облачных ресурсах.

## Требования к лицензированию

Используемое ПО не должно требовать обязательной технической поддержки лицензий.

Программное обеспечение не должно требовать установки дополнительных программных средств, за исключением WEB-браузера и распространенных плагинов.

Процесс эксплуатации Системы не должен требовать от Заказчика приобретения и установки каких-либо дополнительных лицензируемых программных средств, кроме приобретаемых Заказчиком в рамках настоящего ТЗ.

Приобретаемые лицензии на Систему должны быть бессрочными и не зависеть от кол-ва пользователей, устройств и других показателей. Действие лицензий не должно зависеть от приобретения технической поддержки Заказчиком на протяжении всего срока действия лицензий.

## Требования к навигации Системы

Система должна обеспечивать:

• доступ к перечню курсов, к которым пользователь может получить доступ, с возможностью перехода на страницу описания соответствующего курса и к самому курсу;

• доступ к списку ближайших событий в системе с возможностью перехода на страницу описания события, а также к полному списку событий, связанных с образовательным процессом;

• возможность самостоятельного добавления пользователем необходимых курсов, программ и очных мероприятий в план обучения (саморегистрация),

• интуитивно понятный поиск мероприятий по разным критериям (не ограничиваясь, но включая: филиал, дата, тренер, название, тема).

• наличие ссылки на страницу своего профиля;

• наличие ссылки на страницу конструктора курсов и его составляющих (конструктор тестов, опросов, материалов, заданий для пользователей, кому доступна такая функциональность в соответствии с ролью);

• наличие ссылки на страницу модуля организации и проведения вебинаров и/или записи вебинаров (для пользователей, кому доступна такая функциональность в соответствии с ролью);

• наличие ссылки на страницу модуля организации и проведения мероприятий (для пользователей, кому доступна такая функциональность в соответствии с ролью);

• наличие ссылки на страницу конструктора обучающих программ (для пользователей, кому доступна такая функциональность в соответствии с ролью).

## Требования к настройке прав доступа к Системы

В Системе должен быть реализован конфигуратор настраиваемых ролей:

* Суперадминистратор – доступны все функции системы, включая настройки компании.
* Администратор – обладает доступом почти ко всем функциям административной части, кроме распределения уровней доступа.
* Руководитель – руководитель подразделения, проекта или компании. Имеет ограниченный доступ к административной части, где он может согласовывать обучение подчиненных, назначать материалы / развивающие задачи в учебный план сотруднику и видит информацию по бюджету своего отдела.
* Пользователь – линейный сотрудник, который может добавлять материал в базу знаний (на модерацию), рекомендовать коллегам, оставлять отзывы и давать оценку пройденным материалам, подавать заявки на обучение и обладает доступом только к пользовательской части.

Пользователи могут иметь разные роли в разных аккаунтах. В рамках одного аккаунта могут иметь доступ к кабинету обучающегося и куратора курса.

Система должна обеспечивать возможность настройки кастомизируемых ролей.

Система должна обеспечивать возможность разделения пользователей на отдельные группы как полностью автоматически (импорт из файла по установленной форме) на основании заданных параметров, так и вручную куратором с соответствующими правами доступа.

## Требования к функционированию Системы

Система должна обеспечивать:

* хранение не менее чем 5000 курсов;
* хранение данных о результатах освоения всех курсов не менее чем для 10 000 уникальных пользователей Заказчика (до 200 000 записей из расчета на 10 000 уникальных пользователей);
* работоспособности при пиковой нагрузке единовременного доступа 7500 пользователей;
* времени отклика при открытии любой экранной формы не более 2-х секунд при обеспечении рекомендуемых требований к каналу связи (для открытия форм отчетности и статистики для 3000+ пользователей время может быть увеличено до 60 секунд);
* отображение контента в следующих браузерах, версиях после 2020 г. и позднее: Mozila Firefox, Google Chrome, Яндекс.Браузер, Opera, Microsoft Edge, Safari;
* отображение контента на мобильных устройствах под управлением операционных систем iOS (версии 12 и выше) и Android (версии 6 и выше). Допускается использование специализированного мобильного приложения либо отображение в Web-браузере с адаптивным масштабированием.

## Требования к составу обрабатываемых данных

Система должна иметь возможность хранения и обработки следующего состава данных о пользователях и организациях, к которым они относятся:

* ФИО пользователя (текстовое поле);
* дата рождения;
* должность пользователя (текстовое поле);
* полное наименование организации, к которой относится пользователь (из списка);
* краткое наименование организации, к которой относится пользователь (из списка);
* наименование структурного подразделения организации, к которой относится пользователь, а также другие настраиваемые параметры куратором организации (текстовые поля, например, «функция», «подразделение»);
* данные об обучении пользователей (запланированные, текущие и пройденные курсы обучения), сертификаты по результатам обучения.

Осуществление хранения и обработки персональных данных в Системе должно быть обеспечено в соответствии с требованиями законодательства Российской Федерации в области персональных данных.

## Требования к обучающему контенту

Система должна иметь базу встроенных курсов не менее 500 обучающих материалов: курсы, видео, книги, статьи, подкасты по следующим тематикам: менеджмент, лидерство, личная эффективность, ИТ, проектная деятельность, обучение, мотивация, клиенториентированность.

Весь обучающий контент должен быть высокого качества, содержать точные и проверенные данные, а также соответствовать стандартам компании.

Контент должен быть представлен в понятной и доступной форме для всех пользователей, учитывая разнообразный уровень подготовки и опыта.

Обучающий контент должен включать интерактивные элементы, такие как тесты, кейсы и задачи, чтобы обеспечить более глубокое погружение в материал и улучшить усвоение информации.

Контент должен постоянно обновляться для отражения последних изменений в отрасли и технологиях, а также быть релевантным для конкретных рабочих задач и обязанностей пользователей.

Обучающий контент должен быть доступен на различных устройствах, включая компьютеры, и мобильные телефоны

Система должна предоставлять возможность оценки эффективности обучающего контента и его влияния на производительность сотрудников и компании в целом.

Обновление обучающего контента должно осуществляться без перебоев в работе системы.

Система должна предоставлять возможность отслеживать прогресс пользователей в обучении и их успешное освоение материала с помощью системы отчётности и аналитики.

## Требования по безопасности

Система должна отвечать общим требованиям электрической и механической безопасности по ГОСТ 12.2.007.0-75, ГОСТ 25861-83.

Компьютеры и периферийные устройства, входящие в состав Системы должны быть подключены к защитному заземлению, выполненному в соответствии с требованиями ГОСТ 12.2.007.0- 75 и ГОСТ 25861-83.

Система должна соответствовать общим требованиям к обеспечению пожарной безопасности при эксплуатации Системы.

Используемые в системе материалы и органы управления должны соответствовать требованиям ГОСТ 12.2.003-91 и ГОСТ 25861-83.

По уровню звукового давления система должна удовлетворять требованиям ГОСТ 12.1.003-83 и ГОСТ 21552-84.

Доступ в Систему должен быть обеспечен только сотрудникам Заказчика.

Система должна хранить информацию о действиях, которые совершают все пользователи и предоставлять возможность выгрузки логов в текстовый файл. Администратор системы должен иметь возможность настройки уровня логирования действий пользователей.

Передача данных между пользователем и Системой должна осуществляться по безопасному протоколу с применением TLS шифрования.

Протокол взаимодействия (API) должен защищать обмен данными с помощью авторизации и шифрованного соединения.

Система должна предотвращать несанкционированный доступ или модификацию данных.

Система обрабатывает персональные данные физических лиц.

Процессы использования и хранение данных в Сервисе должны отвечать требованиям Федерального закона от 27.07.2006 №152 «О персональных данных».

На стадии проектирования должна быть проведена оценка угроз безопасности информации, реализация (возникновение) которых возможна в разрабатываемой информационной системе персональных данных в соответствии с Методикой ФСТЭК РФ[[1]](#footnote-1), определен уровень защищенности персональных данных в соответствии с ПП-1119[[2]](#footnote-2). На основе установленного уровня защищенности с учетом актуальных угроз безопасности информации сформировать набор мер в соответствии с Приказом № 21[[3]](#footnote-3), необходимых для реализации подсистемы обеспечения информационной безопасности.

Подсистема обеспечения информационной безопасности должна отвечать требованиям к защите персональных данных определенного уровня защищенности.

При сборе персональных данных Исполнитель обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации согласно Федеральному закону от 21.07.2014 №242 «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях».

Если Система собирает, сохраняет либо передает личные сведения, она должна обеспечивать безопасность этих операций с использованием современных надежных методов шифрования (протокола HTTPS).

Исполнитель должен ограничить и контролировать доступ своих сотрудников к информации о пользователях и их персональных данных.

Система, при использовании геоданных, должна получить от пользователя активное согласие (добровольное и осознанное разрешение, которое пользователь может отозвать в любое время) на сбор и использование геоданных. При этом активное согласие пользователя должно запрашиваться отдельно от согласия с политикой конфиденциальности.

Система должна требовать регистрацию или авторизацию пользователя только, если это необходимо для использования Системы (например, чтобы войти под существующим аккаунтом).

Система должна обеспечивать авторизацию пользования с использованием пароля пользователя, а также посредством AD.

Система должна успешно противостоять 10 основным актуальным угрозам безопасности по версии организации OWASP и не иметь критических уязвимостей.

Система не должна устанавливать и использовать другие приложения или неинтегрированные сторонние модули без разрешения пользователя.

Система не должна содержать или включать вредоносное программное обеспечение, в том числе программы-трояны и шпионы.

Система должна использовать надежные, подтвержденные платформой криптографические алгоритмы и не реализовывать собственных алгоритмов.

Система должна соответствовать требованиям Политики информационной безопасности, действующей в группе компаний ПАО «Т Плюс».

Система, все ее компоненты и обновления должны соответствовать Требованиям по информационной безопасности к Web разработке, содержащимся в Приложении №2.

## Требования к исполнителю при осуществлении удаленного доступа к инфраструктуре заказчика

* + 1. Исполнитель предоставляет перечень IP-адресов, принадлежащих исполнителю, с которых планируется производить удаленное подключение.
    2. Исполнитель обеспечивает выполнение условия, что все ресурсы, с которых осуществляется удаленное подключение, в том числе АРМ пользователя и другие технические средства и информационные сервисы, географически размещены на территории Российской Федерации.
    3. При осуществлении удаленного подключения стороннего пользователя к объектам информационной или технологической инфраструктуры Общества посредством не принадлежащего Обществу компьютера или иного средства вычислительной техники (ноутбук, мобильное устройство, далее – оборудование), если это предусмотрено Техническим заданием на работы, такое оборудование должно соответствовать следующим требованиям:

• на оборудовании должно быть установлено лицензионное общесистемное программное обеспечение, находящееся на поддержке производителя;

• на оборудовании должны быть установлены последние обновления для общесистемного программного обеспечения, включая обновления безопасности;

• на оборудовании должно быть установлено и функционировать средство антивирусной защиты, включённое в Единый реестр российских программ для ЭВМ и БД, с актуальными антивирусными базами (дата обновления не старше 7 дней);

• отчет о полной проверке средством антивирусной защиты текущего состояния оборудования (дата отчета не старше 7 дней) не должен содержать событий выявления ВПО или иных событий безопасности.

Подписать соглашение о конфиденциальности и неразглашении информации (NDA).

* + 1. Удаленный доступ сторонних пользователей к информационным и/или технологическим ресурсам Общества, являющимся значимыми объектами критической информационной инфраструктуры (далее – ЗОКИИ), запрещен. В случае необходимости проведения работ на ЗОКИИ, подключение сторонних пользователей к таким объектам и их компонентам допускается только локально на территориальных площадках Общества.
    2. Для организации удаленного доступа используется решение, определенное Заказчиком.
    3. Работники Исполнителя, которым предоставлен удаленный доступ может использовать его только для выполнения своих служебных обязанностей.
    4. Авторизация работника Исполнителя должна осуществляться с учетной записью, выданной Заказчиком, принадлежащей этому работнику. Получение доступа к сервисам Заказчика под чужой учетной записью не допускается и влечет регистрацию инцидента ИБ с последующим расследованием.
    5. Решение, определенное Заказчиком для организации удаленного доступа, является службой, контролируемой Исполнителем. Это значит, что Исполнитель ответственен за выбор провайдера услуг Интернет, координацию установки оборудования и ПО, оплату соответствующих тарифов.
    6. Оборудование, с которого Исполнитель осуществляет доступ к ресурсам Заказчика, настраивается Исполнителем.
    7. Работник Исполнителя не должен допускать неавторизованного доступа других пользователей к информационным ресурсам Заказчика.
    8. Запрещается использовать систему удаленного доступа для организации перманентного подключения сторонних сетей, в том числе локальных сетей Исполнителя.
    9. Запрещается подключение к ресурсам Заказчика с IP-адресов, VPN-провайдеров, узлов TOR и подсетей хостинговых компаний, расположенных за пределами РФ.
    10. Заказчик оставляет за собой право принимать адекватные меры с целью защиты своих информационных, программных и системных активов, свою репутацию и инвестиции в ПО и разработанные сервисы при помощи строгих мер контроля и предотвращения нелегитимного использования сети Интернет или удаленного доступа.
    11. Меры защиты могут включать периодические проверки использования удаленного доступа к ресурсам Заказчика, а также меры по ограничению удаленного доступа в случае выявлении нарушений настоящих требований.

## Условия предоставления удаленного доступа

* + 1. Исполнитель должен предоставить чек-лист проведения оценки состояния информационной безопасности (Приложение № 3), на основании которого Заказчик оценивает возможность предоставления удаленного доступа. Исполнитель по запросу Заказчика должен предоставить копии (выдержки) документов, указанных в чек-листе проведения оценки состояния информационной безопасности.
    2. По согласованию с Исполнителем, Заказчик с помощью технических средств может проводить проверки сведений, указанных в чек-листе, а также следующих требований, предъявляемых к оборудованию (компьютер, ноутбук, мобильное устройство) Исполнителя, которое используется для удаленного подключения:
* на оборудовании должно быть установлено лицензионное общесистемное программное обеспечение, находящееся на поддержке производителя;
* на оборудовании должны быть установлены последние обновления для общесистемного программного обеспечения, включая обновления безопасности;
* на оборудовании должно быть установлено и функционировать средство антивирусной защиты, включённое в Единый реестр российских программ для ЭВМ и БД, с актуальными антивирусными базами (дата обновления не старше 7 дней);
* отчет о полной проверке средством антивирусной защиты текущего состояния оборудования (дата отчета не старше 7 дней) не должен содержать событий выявления ВПО или иных событий безопасности.

1. **Требования к функциям системы**

## Требования к Системе

Перечень функциональности системы зафиксирован в Приложении 1 к настоящему ТЗ «Функциональная спецификация».

## Требования к лингвистическому обеспечению Системы

Интерфейс системы должен быть построен на русском языке.

## Требования к уровням доступа и полномочий

В системе должна быть реализована гибкая ролевая модель, позволяющая настраивать разрешения для пользователей, ролей или групп пользователей на отдельные

* действия и операции в системе;
* объекты управления (курсы, тесты и т.п.);
* сочетание операций и действий.

1. **Требования к технической поддержке и сопровождению**

## Требования к техническому сопровождению

Исполнителем должна быть предусмотрена гарантийная поддержка системы, переданной Заказчику по результатам выполнения работ согласно настоящему Техническому заданию. Исполнитель должен гарантировать качество и надежность функционирования Системы не менее 12 (двенадцати) месяцев с даты завершения всех работ по внедрению Системы в рамках настоящего ТЗ.

Исполнителем должна быть предусмотрена техническая поддержка системы, переданной Заказчику по результатам выполнения работ согласно проектной документации Системы. Исполнитель должен обеспечить техническую поддержку Системы с момента внедрения Системы не менее 36 (тридцати шести) месяцев с даты подписания договора.

В рамках гарантийного срока обслуживания Исполнитель обязан:

* консультировать специалистов Заказчика по вопросам эксплуатации, а также устранения ошибок системы в режиме «вопрос-ответ» с помощью специального сервиса в системе. В экстренных случаях для связи может быть использован телефон;
* устранять ошибки удаленно. В случае невозможности устранения ошибки Исполнителем удаленно или силами Заказчика в соответствии с консультациями Исполнителя, Исполнитель в течение одного рабочего дня с момента получения от Заказчика претензии с описанием ошибок направляет своего представителя к Заказчику для устранения указанных ошибок;
* поставлять новые версии программного обеспечения, произведенные в период гарантийного обслуживания;
* поставлять новые версии встроенных курсов, актуализированных в период технической поддержки.

В рамках срока технической поддержки Исполнитель обязан:

* консультировать специалистов Заказчика по вопросам эксплуатации, а также устранения ошибок системы в режиме «вопрос-ответ» по телефону, электронной почте и с помощью специального сервиса в системе;
* устранять ошибки удаленно. В случае невозможности устранения ошибки Исполнителем удаленно или силами Заказчика в соответствии с консультациями Исполнителя, Исполнитель в течение одного рабочего дня с момента получения от Заказчика претензии с описанием ошибок направляет своего представителя к Заказчику для устранения указанных ошибок;
* поставлять новые версии встроенных курсов, актуализированных в период технической поддержки;
* поставлять новые версии программного обеспечения, произведенные в период технической поддержки.

Ошибками в работе системы считается отклонения в работе Системы относительно требований, зафиксированных в настоящем Техническом Задании и прочей документации, разработанной в рамках Проекта, а также документации, описывающей работу системы, разработанной Исполнителем ранее и размещенной на справочном ресурсе Исполнителя.

Гарантийная и техническая поддержка должна включать в себя консультации Заказчика по телефону в рабочее время сотрудниками Исполнителя и устранение недостатков работы Системы, обнаруженных в процессе эксплуатации. Недостатками Исполнитель считает отклонения в работе Системы, относительно требований, зафиксированных Сторонами в Техническом задании.

Исполнитель должен оперативно отвечать на комментарии и вопросы Заказчика, связанные с Системой.

Исполнитель должен оперативно реагировать на критические программные ошибки и уязвимости в Системе и выпускать обновление с устранением этих ошибок и уязвимостей.

Исполнителем должна быть предусмотрена техническая поддержка системы, переданной Заказчику, в течении 36 месяцев с момента внедрения системы.

Исполнитель обязуется не применять штрафные санкции в случае, если заказчик пропускает период времени между действующими договорами технической поддержки. Заказчик имеет право возобновить договор технической поддержки без уплаты дополнительных средств или штрафных санкций. Пропущенные периоды ТП не могут и не должны оплачиваться Заказчиком при возобновлении ТП на всем периоде действия покупаемых лицензий.

## Уровень гарантийного обслуживания и технической поддержки

* + 1. Техническое и информационное сопровождение осуществляется с 10:00 до 19:00 по московскому времени в рабочие дни, определенные законодательством РФ.
    2. В рабочие, выходные, праздничные дни в случае возникновения Аварийных ситуаций (услуги по другим категориям запросов не предоставляются), техническое и информационное сопровождение осуществляется с 00:00 до 23:59 по московскому времени.

|  |  |  |  |
| --- | --- | --- | --- |
| **Категория запроса** | **Описание**  **запроса** | **Рабочие дни, определенные законодательством РФ** | **Выходные и**  **праздничные дни** |
| Аварийный запрос | Проблема доступности Системы, не зависящая от доступности сервера.  Критическая проблема сервиса, влияющая на выполнение бизнес-процесса. | Срок реагирования:  в течение 1 часа с момента поступления запроса.  Срок выполнения:  в течение 8 часов с момента поступления запроса. | Срок реагирования:  1 часа с момента поступления запроса.  Срок выполнения:  в течение 16 часов с момента поступления запроса. |
| Некритический запрос | Недоработки или ошибки, не оказывающие влияния на работу пользователей Системы. | Срок реагирования:  в течение 4 часов с момента поступления запроса.  Срок выполнения:  в течение 40 дней с момента поступления запроса или в сроки, согласованные с Заказчиком. | Обслуживание не производится. |
| Консультация | Срочная | Срок реагирования:  в течение 2 часов с момента поступления запроса.  Срок выполнения:  в течение 8 часов с момента поступления запроса. | Обслуживание не производится. |
| Консультация | Штатная | Срок реагирования:  в течение 4 часов с момента поступления запроса.  Срок выполнения:  в течение 1 рабочего дня с момента поступления запроса или в сроки, согласованные с Заказчиком. | Обслуживание не производится. |

* + 1. В рамках гарантийного обслуживания и технической поддержки, взаимодействие между Заказчиком и Исполнителем должно осуществляться в рамках регламента оказания Технической поддержки и функциональных изменений, разработанного в рамках реализации Системы.
    2. Все задачи должны фиксироваться в Системе учета задач на стороне Исполнителя с предоставлением доступов представителям Заказчика. Система учета задач должна позволять выгрузить все задачи с описанием решения за отчетный месяц и весь срок ведения проектов Заказчика в удобный формат для заказчика (.docx, .pdf, .xlsx).
    3. Каждый месяц Заказчику должны предоставляться выгрузки реестра задач за отчетный месяц по электронной почте, содержащие перечень задач со следующими характеристиками: номер задачи, категория запроса, название задачи, описание задачи, описание результата выполнения задачи, ФИО постановщика задачи (со стороны Заказчика), тип задачи, дата и время постановки задачи, установленный крайний срок задачи Заказчиком по согласованию с Исполнителем, дата и время начала выполнения задачи, дата и время окончания выполнения задачи, комментарий Заказчика.

1. **План график реализации**
   1. Состав и содержание работ по реализации Проекта

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № этапа | Наименование этапа работ | Дата начала | Длительность (рабочие дни) | Отчётная документация |
| 1 | Внедрение системы |  |  |  |
| 1.1 | Поставка лицензии | С момента подписания договора | Не позднее 14 календарных дней | Сайзинг, инструкция по установке, технический проект на Систему, модель угроз информации Системы, частный технический проект на подсистему защиты информации. |
| 2 | Настройка и ОПЭ системы |  |  |  |
| 2.1 | Настройка корпоративной авторизации, синхронизация с 1С, кастомизация, загрузка данных, настройка структуры компании, настройка контента, компетенций, автоназначения | С момента окончания 1.1 | 47 дней | инструкции по настройке |
| 2.2 | Проведение работ по общему тестированию и устранению замечаний перед ОЭ | С момента окончания 2.1 | 35 дней | Методика ПСИ, протокол ПСИ, журнал устранения замечаний, методика проведения ОПЭ |
| 2.3 | Написание пользовательской документации по работе с внедренной Системой | Одновременно с 2.2 | 35 дней | Инструкции пользователей и администратора, ролевая модель, регламент ТП. |
| 2.4 | Опытная эксплуатация, сопровождение сотрудников | С момента окончания 2.3 | 20 дней | Протокол проведения ОПЭ |
| 2.5 | Консультирование пользователей по работе с Системой | Одновременно с 2.4 | 20 дней | Журнал обращений, записи вебинаров, график обучения |
| 3. | Техническая поддержка |  |  |  |
| 3.1 | Техническая поддержка Системы (*включена в стоимость внедрения Системы*) | С момента окончания 2.4 | 1 календарный год | Журнал обращений |
| 3.2 | Техническая поддержка Системы | С момента окончания 3.1 | 2 календарных года | Журнал обращений |

* 1. Порядок контроля и приемки работ

Приемка результатов выполнения работ поэтапно и оформляется Актом сдачи-приемки работ по факту выполнения полного объема работ по этапу. Основанием для составления и подписания Акта сдачи-приемки по этапу является передача Исполнителем результатов выполнения работ в соответствии с условиями Договора и утвержденных сторонами соответствующего Акта сдачи-приемки работ.

Ежегодно должна предоставляться ТП в виде сертификата на услуги технической поддержки Системы общий срок оказания ТП по контракту - 3 года (согласно п.3.1 плана графика раздела 5.1). Сертификаты ТП предоставляются отдельно на каждый год и должны активироваться последовательно – каждый последующий год – после окончания сертификата на предыдущий год. Сертификат на 1-й год ТП Системы должен быть активирован по истечении 12 месяцев с даты поставки. Действие сертификатов отсчитывается с даты их активации

Недостатки реализации оформляются как выявленные отклонения от настоящего Технического задания и документации, являющейся принятым Заказчиком результатом оказания услуг по Проекту.

* 1. Требования к результатам работ

В рамках реализации Проекта Исполнитель должен обеспечить нижеследующее:

* Подготовку и согласование с Заказчиком детализированного плана-графика реализации проекта не позднее **3 календарных дней** с даты подписания договора. План-график работ должен включать в себя основные этапы работ и все работы внутри каждого из этапов. План-график работ регламентирует этапы работ и все работы внутри каждого из них, фиксирует результат по каждому пункту работ и является приложением к Договору.
* Подготовку программы обучения сотрудников Заказчика по поддержке Системы.
* Разработку инструкций пользователя и обучающих материалов для сотрудников службы технической поддержки Заказчика.
* Документация должна быть передана Заказчику в электронном виде по результатам ее согласования. Каждый документ должен проходить последовательно два этапа – согласование и утверждение Заказчиком. Исполнитель должен передать Заказчику всю документацию, обозначенную в настоящем разделе и разделе 5 настоящего ТЗ.
* Приемка Системы осуществляется Заказчиком по результатам приемо-сдаточных испытаний.
* Система вводится в промышленную эксплуатацию при отсутствии ошибок и сбоев, выявленных в процессе тестирования и опытной эксплуатации.
* Все компоненты Системы должны иметь документацию, описывающую внутреннее устройство и администрирование. Данная документация так же должна быть передана Заказчику.
* Исполнитель один раз в неделю предоставляет Заказчику отчет о ходе выполнения работ, демонстрирует результат проведенных работ и проводит совместное обсуждение выполненных и предстоящих работ.
  1. Требования к организации работ
     1. Сроки начала и окончания работ по каждому из этапов определяются планом-графиком работ.
     2. Все производимые работы должны соответствовать действующим нормам и правилам техники безопасности, пожаробезопасности, а также охраны окружающей среды.
     3. В ходе выполнения работ все согласования и разрешения, необходимые для организации работ и взаимодействия с внешними контрагентами, обеспечивает Заказчик.
     4. Для создания условий функционирования, при которых гарантируется соответствие внедряемой Системы требованиям, содержащимся в настоящем ТЗ, и возможность эффективного использования, в организации Заказчика должен быть проведен комплекс мероприятий по подготовке к вводу Системы в действие.
     5. Силами Исполнителя в срок до перевода Системы в опытную эксплуатацию должно быть проведено консультирование сотрудников Заказчика по работе с Системой. Формат консультирования – вебинар.
     6. Обязательные условия для начала тестирования и приемки работ:
* готовность всей необходимой документации;
* готовность Системы для функционального тестирования;
  + 1. Применяются следующие критерии успешности тестирования:
* Функциональность проверена (верифицирована) на соответствие ее реализации техническим и функциональным требованиям;
* Все запланированные виды тестирования выполнены в полном объеме;
* Все тестовые сценарии, подготовленные для тестирования Системы, выполнены со статусом "Успешно" (отсутствуют тестовые сценарии, которые не запускались вообще или выполнены не полностью);
* Для всех обнаруженных ошибок заведены дефекты в системе баг-трекинга, представляемой Исполнителем;
* Отсутствуют неисправленные дефекты;
* Получено подтверждение от Заказчика для неисправленных дефектов о приемлемости системы для использования с указанными дефектами или оговорена предполагаемая дата их исправления;
* Приемочное тестирование выполнено Заказчиком и официально признано успешным.
  + 1. Работы считаются успешно выполненными, если выполняются все нижеприведенные условия:
* Все разработанные проектные документы согласованы и утверждены Заказчиком;
* Результаты выполненных работ соответствуют заявленной проектной документации;
* Результаты выполненных работ переданы Заказчику;
* Работы выполнены своевременно, соответствуют срокам выполнения;
* На ПСИ не обнаружены дефекты высшего и высокого приоритета. Дефекты высшего и высокого приоритета должны быть исправлены Исполнителем не более чем за десять рабочих дня с момента предоставления Заказчиком списка дефектов. Дефекты среднего и низкого приоритета должны быть исправлены Исполнителем не более чем за двадцать рабочих дней с момента предоставления Заказчиком списка дефектов.
  + 1. Критерии для определения приоритета дефекта:

|  |  |
| --- | --- |
| Приоритет | Ошибка |
| Высший приоритет | Несоответствие настроенного функционала заявленным требованиям настоящего ТЗ  Ошибка, приводящая к потере или повреждению данных в базе данных.  Ошибка, блокирующая бизнес-процесс или приводящая к неправильному результату.  Ошибка, приводящая к зависанию или падению приложения и/или Системы.  Ошибка, которая не позволяет установить, запустить, осуществить вход в систему или продолжить дальнейшую работу с системой. |
| Высокий приоритет | Система игнорирует права доступа и/или другие настройки системы безопасности.  Производительность системы не позволяет выполнить и/или завершить выполнение бизнес-процесса. Производительность системы не удовлетворяет заявленным требованиям.  Непредсказуемое поведение системы при выполнении бизнес-процесса, которое происходит часто, но не приводит к потере и/или повреждению данных. |
| Средний приоритет | Ошибка, которая возникает редко, но не приводит к падению системы и/или зависанию системы.  Система производит не правильные сообщения об ошибках, и/или сообщения об ошибках отсутствуют в необходимом объеме.  Ошибка пользовательского интерфейса, которая вызывает неудобства в работе, но при этом позволяет выполнить шаг или действия бизнес-процесса. |
| Низкий приоритет | Ошибка пользовательского интерфейса, которая не затрудняет работу пользователя с модулем и/или системой. К таким ошибкам относятся: грамматические ошибки, перерисовка экрана, скроллинг, сортировка и т.д.  Другие ошибки, не описанные выше. |

* + 1. Исполнителем должны быть произведены работы по переносу продуктовой версии Системы на сервер Заказчика и/или предоставление документации с инструкциями по переносу тестовой среды на продуктовую силами Заказчика. В случае обнаружения дефектов после переноса системы на сервер Заказчика, должны быть произведены работы по их устранению.

1. Порядок контроля и приемки работ

## Виды, состав, объем и методы испытаний Системы

По итогам работ по внедрению и настройке Системы Исполнителем подготавливаются проекты документов и, затем, проводятся испытания и приемка.

Испытания и приемка проводятся в соответствии с ГОСТ Р 59792-2021 «Информационные технологии. Виды испытаний автоматизированных систем».

По итогам выполнения работ проводятся:

* приемочные испытания;
* опытная эксплуатации.

Испытания проводятся по разработанной Исполнителем, и согласованной с Заказчиком, программе и методике испытаний. Способ проведения испытаний определяется по согласованию с Заказчиком.

## Общие требования к приемке работ по стадиям

Испытания Системы должны представлять собой процесс проверки реализации заданных функций Системы, определения и проверки соответствия настоящего ТЗ, количественных и (или) качественных характеристик Системы, выявления и устранения недостатков в действиях Системы, в разработанной документации.

Для Системы должны проводиться следующие виды испытаний:

* проведение приемочных испытаний;
* проведение опытной эксплуатации.

Испытания проводятся комиссией, формируемой Заказчиком на основании распорядительного документа, который должен определять состав комиссии проведения испытаний, порядок ее работы, место и сроки проведения испытаний. Дата проведения испытаний может быть назначена Заказчиком после завершения этапа работ.

В состав комиссии включаются представители организаций Заказчика и Исполнителя, а также специалисты, привлекаемые Заказчиком.

Приемочные испытания Системы проводят для определения соответствия Системы настоящему ТЗ и решения вопроса о возможности приемки Системы в промышленную эксплуатацию.

Приемочные испытания Системы должны проводиться в соответствии с Программой и методикой приемочных испытаний. Программа и методика приемочных испытаний должна быть разработана Исполнителем и согласована с Заказчиком. Результаты испытаний фиксируются в Протоколе проведения приемочных испытаний с фиксацией решения о переводе Системы в опытно-промышленную эксплуатацию.

Все обнаруженные недостатки в функционировании и в документации Системы, выявленные в процессе испытаний, устраняются Исполнителем.

# Приложение № 1 к Техническому заданию

**Функциональная спецификация**

| **№** | **Требование** | **Параметры** |
| --- | --- | --- |
| 1 | Интерфейс | Отображение каталога курсов и других элементов системы для удобства пользователей: курсы / вебинары / очные мероприятия, фильтры для поиска нужных события/мероприятий (по характеристикам, по названию, по компетенциям, по датам) |
| Размещение характеристик продукта как на центральной витрине/каталоге, так и на странице курса: промо-ролик, описание, продолжительность, автор, рейтинг/отзывы. Возможность найти материал, максимально приближенный к требованиям пользователя по системе тегов, навыков, типу материала, области развития, ключевым словам и т.п. |
| Встроенный конструктор портала (отображения новостей, каталога, контактов, календаря, регистрации) |
| Отображение календаря мероприятий и наличие фильтров для поиска нужных событий / мероприятий |
| Простота навигации для пользователя по платформе, интерфейс должен быть интуитивно понятным пользователю (user friendly). |
| 2 | Регистрация в системе | Возможность массового импорта/экспорта пользователей – импорт пользователей автоматизирован, есть массовая регистрация через API |
| Возможность ручного добавления нового пользователя администратором |
| Возможность самостоятельной регистрации пользователя на нужный курс/мероприятие/программу и т.д. |
| Возможность настроить свободную или модерируемую регистрацию для каждого курса или события. |
| Фильтрация пользователей по всем имеющимся полям |
| Модерация заявок на обучение |
| Общий принцип предоставления прав доступа – через логин пользователя (login= корпоративный email сотрудника) |
| 3 | Интеграция (1C, Active Directory, вебинарные площадки) | Возможность интегрироваться с внутренней базой сотрудников для автоматического создания и обновления профилей сотрудников |
| Возможность импорта данных через шаблоны для стандартных процессов, например, загрузки excel файлов с историей обучения, статусами по регистрации, списками вопросов и ответов для тестирований, списками курсов и т.п. |
| Отображение в системе профилей пользователей с основными данными по сотруднику |
| Возможность интегрироваться с внешними сервисами по API для проведения онлайн вебинаров |
| 4 | Процессы и задачи | События/условия задач - регистрация в системе, дедлайны курса, прогресс прохождения |
| 5 | Управление пользователями | Ролевой принцип разграничения прав доступа |
| Создание и управление обязательными для заполнения доп. полями пользователя |
| Участник – обучение по назначенным курсам; просмотр доступной части базы знаний, электронной библиотеки; просмотр расписания мероприятий; просмотр и редактирование профиля с личными данными; просмотр статистики и результатов обучения по текущим и ранее пройденным курсам; просмотр ленты новостей; чаты с куратором, преподавателем и тех.поддержкой; просмотр рейтингов; выгрузка сертификата о прохождении обучения; функционал добавления собственного материала любого формата в общую базу знаний компании (с предварительной модерацией со стороны администратора); функционал рекомендаций понравившегося контента коллегам; отзывы и оценка пройденных материалов; подача заявки на обучение; возможность создавать и редактировать собственный индивидуальный план развития/обучения, возможность прохождения диагностики навыков. |
| Тьютор – проверка и выставление оценок по заданиям с открытым вариантом ответа; чаты с участниками, с технической поддержкой; просмотр и редактирование доступной части базы знаний |
| Куратор – чаты с участниками; просмотр статистики и результатов обучения курируемых групп участников; работа с задачами в процессах; создание и редактирование мероприятий; модерация заявок на обучение |
| Руководитель – просмотр статистики и результатов/прогресса обучения подведомственных групп/своих сотрудников; согласование обучения подчиненных; возможность назначения материалов и развивающих задач в учебный план сотруднику, доступ ко всем учебным планам сотрудников, которые относятся к его отделу/функции |
| Разработчик курсов – создание, редактирование материалов в базе знаний и курсов |
| Супердминистратор – полные права доступа; выдача прав всем пользователям; возможность блокировки отдельного пользователя. Управление профилем сотрудника (просмотр, назначение обучения, удаление обучения, просмотр истории обучения и т.д.); массовая регистрация/назначение обучения на пользователей; возможность автоматического назначения обучения на основе заданных правил и возможность настраивать данные правила; возможность создавать и редактировать индивидуальный план развития сотрудника, управлять планом развития сотрудника (добавлять/убирать обучения, фиксировать прохождение обучения и т.д.); возможность создавать и редактировать теги для курсов/тренингов/программ; настройка и управление процессом согласования заявок на обучение, управление списками регистрирующихся на мероприятие с возможностью регистрировать их и менять статусы; создание программы собранной из тренингов/курсов/ссылок/документов и т.д. (в том числе, внешних) |
| Администратор – управление профилем сотрудника (просмотр, назначение обучения, удаление обучения, просмотр истории обучения и т.д.); массовая регистрация/назначение обучения на пользователей; возможность автоматического назначения обучения на основе заданных правил и возможность настраивать данные правила; возможность создавать и редактировать индивидуальный план развития сотрудника, управлять планом развития сотрудника (добавлять/убирать обучения, фиксировать прохождение обучения и т.д.); возможность создавать и редактировать теги для курсов/тренингов/программ; настройка и управление процессом согласования заявок на обучение, управление списками регистрирующихся на мероприятие с возможностью регистрировать их и менять статусы; создание программы собранной из тренингов/курсов/ссылок/документов и т.д. (в том числе, внешних) |
| Возможность вести базу внутренних тренеров |
| Возможность создать пустой элемент для внесения статусов администратором за определенную активность сотрудника (например, участие во внешнем мероприятии) |
| Возможность гибких настроек доступа к созданию, редактированию, управлению курсами |
| Наличие у пользователей личной страницы/личного кабинета, в котором представлены планы обучения (ИПР), персональная информация о пользователе с фотографией, перечень навыков сотрудника, загруженный сотрудником материал, рекомендованный сотрудником материал, статистика обучения, рекомендации обязательного/рекомендуемого обучения.  Для роли руководитель: доступ к статистике обучения, назначение обязательного/рекомендуемого обучения и т.д. |
| 6 | Мобильная версия | Аккаунт участника |
| Просмотр контента при отсутствии интернета с помощью функции предварительной загрузки |
| 7 | Курсы и программы | Наличие конструктора курсов (учебные материалы + тесты/задания +опрос/отзыв) и программ обучения (верстка сложносоставных образовательных программ с модулями разной продолжительности и форматов, типа курс+курс+...) |
| Возможность вставки страниц, созданных в Tilda |
| Редактор создания статей или лонгридов, позволяющий работать с изображениями, добавлять видео, форматировать текст, загружать презентации в формате pdf. как часть курса |
| Организация синхронного (живого) обучения, включая сбор заявок, регистрацию, рассылку напоминаний участника, аналитика по результатам |
| Возможность возобновления прохождения курса пользователем с места прерывания курса или сначала |
| Проигрывание загруженных файлов во встроенном плеере с постраничным просмотром и зумом изображения |
| Отсутствие фонового режима в работе курсов и элементов курсов (при закрытии окна с обучением, видео курса останавливается) |
| Возможность добавления материалов для скачивания к каждой части курса |
| Навигация внутри курса: свободная / последовательное открытие / интервальное открытие / стоп уроки |
| Возможность разделить комплексный курс/программу на отдельные модули и загрузить каждый модуль в формате отдельного курса в базу знаний, чтобы сделать доступным прохождение отдельного модуля без необходимости проходить весь курс. |
| Подсчет прогресса обучения, возможность при необходимости засчитать обучение на любом моменте прогресса |
| Возможность назначения обязательного прохождения курса до конца (нельзя завершить, не пройдя весь) |
| Балльная система оценивания |
| Возможность пересмотра контента пройденного курса/тренинга |
| Наличие опросов в конце курса (выбор ответа, свободный комментарий, лайк/дизлайк) |
| 8 | Типы учебных материалов | Аудио mp3. |
| Видео mp4. mov. |
| Html-страницы |
| Справочные документы (PDF, DOC, XLS, PPT) |
| Встроенные ресурсы (YouTube, Vimeo, LearningApps, Google Drive, Google Forms, Typeform) |
| SCORM |
| 9 | Конструктор создания курсов в форматах SCORM | Возможность публикации/загрузки курсов в данном формате |
| Встроенный плеер SCORM курсов с импортом всех форматов и проигрывание на платформе любого из загруженных SCORM-курсов как отдельного курса или части сложносочиненного курса, сформированного из разных форматов. При импорте для каждого курса возможна опция последовательного или свободного прохождения |
| 10 | Типы тестирования | Единичный выбор |
| Множественный выбор |
| Упорядочивание |
| Сопоставление |
| Открытый вопрос |
| Вопрос с автопроверкой |
| Заполнение пробелов |
| Возможность подгрузить вопрос в виде аудио/видео файла |
| 11 | Настройки тестирования | Возможность выставить проходной балл |
| Возможность выставить вес в количестве баллов за правильный ответ |
| Регулирование количества попыток прохождения |
| Регулирование времени прохождения |
| Возможность настроить видимость правильных ответов |
| Импорт / экспорт результатов тестирования в xls. |
| Сбор показателей качества тестовых заданий: сложность, процент правильных ответов |
| Встроенный конструктор отчетов, который позволяет формировать отчеты в требуемом виде и форматах xls. и PDF. |
| Возможность сбора и анализа данных, фильтрации и сортировки полученных результатов, работы со статистикой в различных срезах |
| Загрузка вопросов в систему в формате xls. |
| Возможность создания перечня вопросов и формирования случайной выборки из общего списка вопросов |
| 12 | Задания | Задания открытого типа с возможностью прикрепления файлов |
| Проверка и оценка ответов тьютором/руководителем/администратором/другой ролью, назначенной для конкретного типа заданий |
| 13 | Мероприятия | Конструктор для уведомления и отображения в календаре: очная встреча / вебинар, тема, описание, организатор, обложка, продолжительность, ссылка на онлайн встречу / место проведения, вместимость |
| Учет посещаемости |
| Конструктор для составления расписания очных занятий с учетом свободных помещений и нагрузки тренеров |
| 14 | Документы об окончании обучения | Конструктор электронных сертификатов (с автозаполнением параметров – ФИО участника, наименование курса, длительность курса, дата завершения) |
| 15 | Чат | Чат между участником и тьютором при выполнении задания с открытым типом ответа |
| Чат между участником и куратором по организационным вопросам |
| 16 | Настройки обращений | Возможность отправки приглашений зарегистрироваться на мероприятие (очное мероприятие, вебинар) |
| Приглашение изучить курс, материалы, загруженные в систему |
| 17 | Уведомления | Редактирование текстов готовых шаблонов уведомлений (нотификаций) при наступлении событий в системе:   * о регистрации на вебинар/сессию/очное мероприятие * об изменении статуса участия в очном вебинаре/очном обучении * о проверке заданий тьютором * о назначении курса/обучения * о прохождении обучения * о дедлайнах в курсе * о записи на мероприятие * о сроке завершения курса * нотификацию по форме обратной связи после завершения программы |
| Возможность настраивать критерии отправки уведомлений (например, отсутствие уведомления руководителю, участнику - при внесении данных по прошедшему мероприятию, когда не требуется уведомление, включать/выключать нотификацию) |
| 18 | Отчетность и аналитика | Дата регистрации участника в аккаунте |
| Дата последней активности в аккаунте |
| Количество пройденных курсов и мероприятий |
| Прогресс прохождения каждого курса (% прохождения) |
| Количество назначенных курсов и мероприятий |
| Количество верных /неверных ответов по каждому вопросу теста |
| Отчет по ответам на открытые вопросы |
| Выгрузка отчетов по пользователю, группе пользователей, курсу, программам с выбором диапазона дат, назначенных тренингов, статистике просмотров, времени нахождения на плаформе и т.д. |
| Возможность выгрузить отчетность на текущую дату и за выбранный период времени |
| Возможность как отправки отчетов на электронную почту себе/другому лицу по email из системы в виде файлов (.xlsx, .csv), так и загрузки без отправки на электронную почту |
| Выгрузка отчета по всем мероприятиям конкретного участника (очные мероприятия, дистанционные курсы) |
| Возможность настроить кастомный отчет с необходимыми полями (у определенных ролей, например, только у администратора) |
| Возможность управления выгрузкой отчетов (например, автоматическая периодическая выгрузка отчета, отложенная выгрузка отчета). |
| Возможность представления отчетной информации в виде дашбордов |
| 19 | Компетенции | Создание справочника компетенций |
| Присвоение компетенций при завершении курса |
| Назначение компетенций на курс |
| Распределение компетенций по учебным материалам и оценочным заданиям курса |
| Отслеживание тьютором освоения компетенций участниками курса |
| Отслеживание освоение компетенций участником в своем профиле |
| Возможность создавать группы сотрудников по определенным критериям на основе характеристик профилей/требуемых предустановленных компетенций |
| 20 | Группы | Вручную объединение участников по определенным признакам |
| Условия для автораспределения участников в группы |
| 21 | База знаний | Размещение учебного материала с возможностью размещения, сортировки и фильтрации, по ключевым словам, навыкам, длительности, формату, авторству |
| Возможность выставления оценок материалу, рекомендации его другим пользователям |
| Количество образовательного контента, загруженного в Систему, не менее 500 обучающих материалов (курсы, видео, книги, статьи, подкасты) по тематикам: менеджмент, лидерство, личная эффективность, ИТ, проектная деятельность, обучение, мотивация, клиентоориентированность. |
| 22 | Лента новостей | Размещение новостного материала, разграничение контента по ролям пользователей, комментарии, лайки |
| 23 | Брендирование | Замена домена, логотипа, оформление платформы в цветах фирменного стиля (кнопки, визуальные элементы), фоновая страница для входа (кастомизация приветственного текста при входе на платформу) |
| 24 | Участие в тендерах | Является резидентом РФ |
| 25 | Конфиденциальность | Гарантия конфиденциальности и целостности передаваемой информации |
| 26 | Доступ пользователей к персонализированным функциям | Доступ только после прохождения аутентификации и авторизации |
| 27 | Доступность | Доступность для самостоятельной работы на устройствах компьютер (через браузер Google Chrome, Microsoft Edge) и Мобильные устройства (операционная система iOS, Android) |
| 28 | Очное обучение / вебинары | Возможность создавать, организовывать/проводить очные тренинги/вебинары на платформе или с размещением ссылки для перехода на внешний ресурс |
| 29 | Бюджетирование и работа с заявками на внешнее обучение | Возможность управлять подачей заявок на обучение и управлять статусами рассмотрения заявок на обучение |
| 30 | Геймификация | Наличие элементов геймификации (значки, баллы, награды) |
| Возможность формировать рейтинг сотрудников по прохождению обучения |
| Возможность выгружать рейтинг сотрудников и контента |
| 31 | Оценка обучения /обратная связь по программам/курсам | Возможность у пользователей оценивать любой контент (ставить лайки/дизлайки, рекомендовать материалы) |
| Рейтинг контента (курсов, тренингов, программ, материалов) на основе лайков/отзывов/просмотров/рекомендаций |
| Возможность у роли администратора создавать и редактировать, выгружать формы обратной связи по тренингу/курсу/тренеру |

# Приложение № 2 к Техническому заданию

**Требования информационной безопасности для Web разработки**

**1. Требования к защите от НСД**

1.1 Компоненты подсистемы защиты от НСД должны обеспечивать:

• идентификацию пользователя;

• проверку полномочий пользователя при работе с системой;

• разграничение доступа пользователей на уровне задач и информационных массивов;

1.2 Протоколы аудита системы и приложений должны быть защищены от несанкционированного доступа как локально, так и в архиве.

1.3 Система должна предотвратить работу с некатегоризированной информацией под сеансом пользователя, авторизованного на доступ к конфиденциальной информации.

1.4 Система должна обеспечивать разделение полномочий администраторов и персонала, обеспечивающего ее функционирование, возможность назначения минимально необходимых прав и полномочий.

**2. Требования к сетевому взаимодействию и каналам связи**

2.1 Защищённая часть системы должна быть отделена от незащищённой части системы межсетевым экраном.

2.2 Данные, передаваемые по сети, шифруются с использованием TLS. Безопасный канал используется для всех сервисов приложения.

2.3 Настройки TLS соответствуют современным лучшим практикам, или максимально приближены к ним, если операционная система не поддерживает рекомендуемые стандарты.

2.4 Приложение верифицирует X.509 сертификаты сервера во время установления защищённого канала. Принимаются только сертификаты, подписанные доверенным удостоверяющим центром (CA).

2.5 В приложении реализован SSL pinning и соединение с серверами, которые предлагают другой сертификат или ключ, даже если они подписаны доверенным центром сертификации (CA) не устанавливается.

2.6 Приложение не полагается на единственный небезопасный канал связи (e-mail или SMS) для таких критических операций, как регистрация и восстановление аккаунта.

2.7 Приложение использует только актуальные версии библиотек для подключения к сети и обеспечения безопасного соединения.

**3. Требования к защите соединений**

3.1 Все клиент-серверные взаимодействия должны осуществляться с использованием защищенного транспортного протокола через TLS версии не ниже 1.2.

3.2 Для принудительного использования HTTPS для всех запросов необходимо использовать strict-transport-security (HSTS) заголовки.

3.3 Используемые Cookie должны быть httponly и ограничены путем и доменом.

3.4 Для веб-приложений необходимо использовать Content Security Policy, разрешающую минимально необходимый перечень источников контента.

**4. Требования к механизмам аутентификации и авторизации**

4.1 Все интерактивные формы HTML должны быть защищены от Cross-Site Request Forgery (CSRF).

4.2 Механизм аутентификации должен быть защищен от атак Brute force, Password spraying и Credential Stuffing – должен быть реализован механизм определения необычно большого количества попыток аутентификации от одного или нескольких источников.

4.3 Парольная политика разрабатываемого приложения должна соответствовать парольной политике Компании. Максимальная длина пароля и количество типов используемых символов не должны быть ограничены. Хранить пароли необходимо с помощью надежных, адаптивных функций хеширования с солью и фактором трудоемкости (задержки), таких как Argon2, scrypt, bcrypt или PBKDF2.

4.4 Использовать при восстановлении пароля эффективные методы восстановления учётных данных и паролей.

4.5 Пароли и другие аутентификационные данные не должны содержаться в исходном коде.

4.6 Пароли и другие аутентификационные данные должны передаваться только через шифрованные и аутентифицированные протоколы.

4.7 Пароли должны обрабатываться необратимыми хэш-функциями при их вводе. Запрещено оперировать паролями в незащищенном виде.

4.8 Аутентификационные и авторизационные данные не должны передаваться на сторону клиента. Это гарантирует невозможность компрометации путем манипуляций программным обеспечением на стороне клиента.

4.9 Пароли и другие конфиденциальные данные, такие как Session IDs и Database IDs, никогда не должны передаваться как URL-параметр в HTTP Get запросах.

4.10 Пароль никогда не должен показываться в открытом виде (при вводе и других формах).

4.11 Для аутентификации в контексте ресурсов, размещенных в корпоративной системе передачи данных, рекомендуется использовать доменную аутентификацию Active Directory. Программное решение должно поддерживать интеграцию со службой каталогов Active Directory в качестве поставщика идентификаций и назначения прав доступа. При использовании протокола LDAP для интеграции с Active Directory передаваемые данные должны быть защищены с помощью протокола TLS (LDAPS).

4.12 В контексте внешних ресурсов информационная система должна поддерживать два типа аутентификации пользователей: с помощью логина/пароля, в случае отсутствия учетной записи пользователя в Active Directory и с использованием корпоративной системы ADFS.

4.13 Аутентификационные данные должны храниться в зашифрованном виде.

4.14 Максимальная длина пароля и количество типов используемых символов не должны быть ограничены.

4.15 В сервисах, опубликованных в сети Интернет, рекомендуется выполнять аутентификацию пользователей на основании стандартов saml, oauth или openid; в качестве поставщика идентификаций для корпоративных пользователей рекомендуется использовать Active Directory Federation Services (AD FS).

4.16 При изменении конфиденциальных данных рекомендуется инициировать повторный процесс аутентификации пользователя.

**5. Требования к управлению сессиями**

5.1 Продолжительность сессии пользователя должна быть ограничена (ограничение по времени бездействия пользователя).

5.2 Механизм установления сессий (Session Management) должен быть защищен от атак на перехват сессии (Session Fixation attacks).

5.3 Длина идентификатора сессии должна быть не менее 128 бит. Идентификатор сессии должен быть абстрактным относительно функционала ПО.

5.4 Должна соблюдаться высокая степень энтропии нумерации сессий, рекомендуется использовать метод случайных чисел.

5.5 Недопустимо передавать идентификатор сессии как часть URL. Рекомендуется использовать параметризированные HTTPS запросы или Cookie.

5.6 Должен обеспечиваться сбор, запись и хранение информации о действиях персонала и администраторов.

**6. Требования к организации ввода данных**

6.1 Вводимые в приложение данные должны подвергаться синтаксической и семантической проверкам, вводимые пользователем данные проверяются, фильтруются и очищаются.

6.2 Должны использоваться надежные механизмы экранирования при передаче вводимых пользователем данных для предотвращения SQL-инъекций. Аналогичный подход необходимо использовать при передаче файлов.

6.3 Все вводимые пользователем или внешними приложениями данные должны рассматриваться как потенциально опасные. Должен быть реализован механизм проверки этих данных на стороне клиента, а затем на принимающей стороне. Проверки должны содержать контроль минимального и максимального размера передаваемых данных, а также их тип.

6.4 Должен проверяться синтаксис выводимых данных на предмет отсутствия спецсимволов для предотвращения XSS-атак

6.5 Необходимо использовать безопасный API, исключающий применение интерпретатора или предоставляющий параметризованный интерфейс, либо использовать инструменты объектно-реляционного отображения (ORM).

6.6 Взаимодействие с приложением по интерфейсу API рекомендуется ограничить доступ по белому списку IP-адресов или иных источников подключения.

6.7 Все общедоступные формы ввода данных должны быть защищены от множественной отправки с помощью капчи.

**7. Требования к механизмам отладки и аудита**

7.1 Сообщения об ошибках не должны содержать конфиденциальной информации, такой как данные пользователя, stack traces, dumps, данные логов и прочее.

7.2 Подробная информация об ошибках (exceptions, stack traces, dumps) должна сохраняться в защищенном месте на стороне сервера и содержать достаточно данных для анализа ошибки командой разработки, расследования инцидентов ИБ работниками Центра ИБ. Набор данных для логирования прорабатывается на этапе проектирования архитектуры и согласовывается с Центром ИБ.

7.3 В информационной системе необходимо использовать контроль целостности журналов аудита важных транзакций для предотвращения подмены или удаления данных.

7.4 В информационной системе необходимо регистрировать сбои и уведомлять администраторов при необходимости (например, если сбои повторяются).

**8. Требования к реализации доступа к файловой системе**

8.1 Для доступа к файловой системе должны использоваться нормализованные и приведенные к корню разрешенного каталога пути.

8.2 Просмотр каталога файловой системы должен быть запрещен для предотвращения раскрытия данных, а также обеспечить отсутствие метаданных файлов (например, \*.git) и файлов резервных копий в корневых веб-каталогах.

**9. Требования к загрузке и хранению пользовательских данных**

9.1 При загрузке определенных типов файлов, должны выполняться проверки их типа и/или расширения.

9.2 Должны быть реализованы проверки загрузки файлов только в разрешенные каталоги.

9.3 Объемы загрузки данных должны быть лимитированы минимально необходимыми.

9.4 Хранилища критичных данных должны шифроваться, в том числе резервные копии.

9.5 Кэширование ответов, содержащих конфиденциальные данные, должно быть отключено.

**10. Требования к интеграции с корпоративными системами**

10.1 Необходимо использовать принцип минимальных привилегий: выполнение кода должно происходить с минимально возможными привилегиями. Разработанные службы не должны запускаться и работать с повышенными привилегиями, кроме случаев, когда это обоснованно, задокументировано и согласовано всеми участниками процесса безопасной разработки.

10.2 Многоуровневая защита (эшелонирование): защита разрабатываемого программного продукта и данных должна осуществляться на всех этапах обработки информации и на всех уровнях ИТ инфраструктуры.

10.3 Шифрование конфиденциальной информации: вся конфиденциальная информация должна храниться в зашифрованном виде.

10.4 Обработка исключений: стандартные действия для методов или запросов должны обрабатывать исключения таким образом, чтобы это не влияло на конфиденциальность, целостность и доступность данных.

10.5 Журнал аудита: должен быть реализован журнал аудита для обеспечения контроля действий пользователей и работы ПО.

10.6 Принцип минимизации данных и принцип ограничения цели: программное обеспечение должно оперировать только необходимыми данными и использовать их только в первоначально определенных целях. Обработка персональных данных должна быть ограничена целью их обработки в соответствии с функциональным назначением ПО. При этом персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки.

10.7 Разработка архитектуры ИТ инфраструктуры должна осуществляться с привлечением работников Центра поддержки инфраструктуры.

10.8 Должны выбираться библиотеки и протоколы актуальных версий с учетом лучших практик в сфере разработки и обеспечения информационной безопасности.

10.9 В корпоративных системах запрещено использовать неподдерживаемые и неактуальные сторонние библиотеки и фреймворки, для которых разработчиком не отслеживаются и не исправляются уязвимости.

10.10 При выборе алгоритма шифрования необходимо руководствоваться требованиями законодательства РФ.

10.11 В случае необходимости использования самописных протоколов в корпоративных системах, их использование должно быть обосновано, задокументировано и согласовано всеми участниками процесса разработки.

10.12 Журналы приложений не должны содержать конфиденциальных данных (учетные данные, токены, и т.п.).

10.13 Все используемые в разрабатываемых продуктах сторонние компоненты должны быть получены из подтвержденных внутренних источников (artifactory) и проверены на уязвимости.

10.14 Программный код разрабатываемого программного обеспечения должен проверяться разработчиком на наличие ошибок программирования и потенциальных уязвимостей перед его переводом в продуктивный режим (code review).

10.15 Запрещено переносить в продуктовую среду результаты разработки (артефакты), в которых были выявлены уязвимости критического, высокого и среднего уровней. Наличие уязвимостей низкого уровня допустимо по согласованию с работниками Центра ИБ и с занесением в технический долг команды разработки.

**11. Требования к безопасности кода**

11.1 При разработке безопасного программного обеспечения командой разработки не должны допускаться ошибки и уязвимости, вызванные:

• Отсутствием необходимого параметра, присвоением параметру неправильных значений, наличием избыточного числа параметров или неопределенных параметров ПО.

• Отсутствием проверки значений, избыточным количество значений, неопределенностью значений, вводимых (входных) данных.

• Отслеживанием пути доступа к каталогу по адресной строке или составному имени и получении доступа к предыдущему или корневому месту хранения данных.

• Возможностью внедрения ссылки на сторонние ресурсы, которые могут содержать вредоносный код. Для файловых систем недостатками являются символьные ссылки и возможность прослеживания по ним нахождения ресурса, доступ к которому ограничен.

• Возможностью выполнения пользователем команд ОС, таких как просмотр структуры каталогов, копирование, удаление файлов и других команд.

11.2 При разработке безопасного программного обеспечения необходимо:

• Исключить возможность внедрения кода в веб-страницы (скрипты, выполняющиеся на стороне пользователя) для получения данных нелегитимными пользователями.

• Исключить возможность внедрения интерпретируемых операторов языков программирования (например, операции выбора, добавления, удаления и другие) или разметки в исходный код веб-приложения.

• Исключить возможность внедрения кода или части кода, приводящего к нарушению процесса выполнения операций.

• Исключить осуществление записи данных за пределами области выделенной для ПО в памяти буфера.

• Контролировать форматную строку функции ввода/вывода.

• Исключить преднамеренное или неумышленное разглашение информации ограниченного доступа.

• Исключить возможность обхода аутентификации, ошибки логики процесса аутентификации, отсутствие запрета множественных неудачных попыток аутентификации, отсутствие требования аутентификации для выполнения критичных функций.

• Исключить хранение информации в незашифрованном виде, ошибки при управлении ключами, использование несертифицированных средств криптографической защиты информации (там, где это обусловлено требования законодательства РФ).

• Предусмотреть функционал проверки правильности формирования запроса (защита от SQL инъекций).

• Исключить переполнение буфера.

• Исключить недостатки проектирования многопоточной системы или приложения, при которой функционирование системы или приложения зависит от порядка выполнения части кода ("Состояние гонки").

• Принять меры по освобождению выделенных участков памяти после использования, отсутствием очистки памяти процессов от сведений ограниченного доступа перед повторным использованием, возможностью повторного использования освобожденной памяти.

**12. Требования к десериализации.**

12.1 Необходимо отклонять сериализованные объекты от недоверенных источников или использовать среды сериализации, допускающей только примитивные типы данных. Если это невозможно, рекомендуется следующее:

• Проводить проверку целостности сериализованных объектов, например, с помощью цифровых подписей, для предотвращения создания вредоносных объектов или подмены данных.

• Использовать ввод строгих ограничений типов при десериализации перед созданием объекта, поскольку ожидаемым является поддающийся определению набор классов.

• Соблюдать изоляцию и запуск кода, осуществляющего десериализацию, в среде с минимальными привилегиями, если это возможно.

• Журналировать исключения и ошибки десериализации, например, непредусмотренных типов входных данных или исключений при десериализации.

• Ограничивать или контролировать входящие и исходящие сетевые подключения контейнеров или серверов, осуществляющих десериализацию.

• Отслеживать десериализацию с предупреждением о фактах продолжительной десериализации.

**13. Требования к актуальности компонентов информационной системы.**

13.1 На все компоненты информационной системы должны быть установлены обновления безопасности.

13.2 Рекомендуется выполнять регулярное обновление компонентов информационной системы не реже одного раза в 3 месяца.

13.3 Обновления должны устанавливаться только из доверенных источников (с официальных сайтов и репозиториев производителей программного обеспечения).

**14. Соблюдение требований законодательства и ЛНА в части конфиденциальных данных (персональные данные, коммерческая, служебная тайна и прочее).**

14.1 Необходимо классифицировать данные, обрабатываемые, хранимые или передаваемые приложением. Определить какие из них являются конфиденциальными. относятся к персональным данным и т.д. согласно законам о неприкосновенности данных, нормативам или бизнес требованиям.

14.2 При разработке безопасного программного обеспечения разработчики ПО должны руководствоваться:

• отраслевыми стандартами безопасного программирования: ISO 15408, ISO 27034-1, ISO TR 24772, Microsoft Security Development Life Cycle, Cisco Security Development Life Cycle, OpenSAMM, OWASP CLASP, ГОСТ Р56920-2016, ГОСТ Р56921-2016, ГОСТ Р56922-2016, ГОСТ Р56923-2016, ГОСТ Р56939-2016.

• Если разрабатываемое ПО предполагает работу с конфиденциальной информацией, разработчик и/или его соисполнители должны подтвердить применение мер по разработке безопасного ПО на всех этапах жизненного цикла (SDLC).

• Процесс разработки должен быть выстроен с учетом лучших практик по организации процесса разработки безопасного ПО (требования регламентов ФСТЭК России, национального стандарта ГОСТ Р 56939-2016, международных стандартов серии ISO/IEC 27000, материалов OWASP, рекомендаций NIST).

# Приложение № 3 к Техническому заданию

**Чек-лист проведения оценки состояния информационной безопасности при взаимодействии с третьими лицами**

Наименование контрагента: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Предмет договора \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Вопросы распространяются на бизнес-процессы, информационные системы, технические и программные средства, которые будут использованы исполнителем для обработки информации ПАО «Т Плюс», его зависимых и дочерних компаний.

Заполняющая сторона гарантирует точность, полноту и достоверность предоставленных ответов.

Дата заполнения: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Кем заполнено (ФИО, Должность): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

| **№ п/п** | **Вопрос** | **Ответ** | **Подтверждающий документ** |
| --- | --- | --- | --- |
| 1 | Каким образом в Вашей организации установлены внутренние требования по информационной безопасности?  В каких областях (например, управление доступом,  учет информационных ресурсов,  управление уязвимостями, защита от вредоносного ПО и т.п.) установлены требования по информационной безопасности?  Как давно пересматривались требования по данным областям? |  |  |
| 2 | Назначено ли в Вашей компании лицо, ответственное за обеспечение информационной безопасности? |  |  |
| 3 | Каким образом в Вашей компании обеспечиваются меры по предотвращению неавторизованного физического доступа посторонних лиц в помещения, используемые для обработки конфиденциальной информации? |  |  |
| 4 | Опишите, каким образом в Вашей компании обеспечивается управление правами доступа, в том числе: | |  |
| 4.1 | Каким образом (общий порядок) выдаются и отзываются права доступа пользователей к информационным ресурсам? |  |  |
| 4.2 | Каким образом контролируется корректность выполнения процедур выдачи и отзыва прав доступа? |  |  |
| 4.3 | Используются ли в вашей компании средства автоматического управления доступом пользователей к информационным ресурсам?  Какие функции реализуют эти средства? |  |  |
| 4.4 | Установлены ли минимальные требования к паролям? |  |  |
| 4.5 | Каким образом в Вашей компании осуществляется управление встроенными учетными записями технических и программных средств? |  |  |
| 5. | Каким образом защищаются рабочие станции и сервера, от вредоносного программного обеспечения? Какова частота обновления антивирусных баз? |  |  |
| 6. | Каким образом в Вашей компании осуществляется регламентирование установки и использования программного обеспечения (неиспользование не разрешенного ПО)? |  |  |
| 7. | Каким образом в Вашей компании осуществляется управление конфигурациями технических средств и программного обеспечения? |  |  |
| 8. | Каким образом в Вашей компании осуществляется управление уязвимостями (анализ и устранение) технических средств и программного обеспечения? |  |  |
| 9 | Каким образом в Вашей компании осуществляется управление (контроль использования, запрет использования в определенных случаях, применяемые стандарты безопасности при настройке, и т.п.) беспроводными сетями? |  |  |
| 10 | Каким образом в Вашей компании осуществляется управление (использование для работы с корпоративными ресурсами, служебные устройства, меры обеспечения защиты при использовании устройства и т.п.) мобильными устройствами? |  |  |
| 11 | Каким образом в Вашей компании осуществляется резервное копирование и восстановление информации? |  |  |
| 12 | Каким образом в Вашей компании доводятся до сотрудников требования по информационной безопасности? |  |  |
| 13 | Каким образом в Вашей компании реализован контроль подключения периферийных устройств к портам рабочих станций и серверов? |  |  |
| 14 | Каким образом в Вашей компании обеспечивается регистрация и мониторинг событий безопасности? |  |  |
| 15 | Каким образом в Вашей компании реализована защита периметра корпоративной сети? |  |  |
| 16 | Каким образом в Вашей компании обеспечивается управление инцидентами информационной безопасности? В какой срок обеспечивается расследование инцидентов? Какие стороны уведомляются в случае обнаружения инцидента? |  |  |
| 17 | Каким образом в Вашей компании уничтожается информация в случае утраты необходимости в её обработке (уничтожение персональных данных или иной конфиденциальной информации)? |  |  |

1. Методический документ «Методика оценки угроз безопасности информации» (утв. ФСТЭК России 5 февраля 2021г.). [↑](#footnote-ref-1)
2. Постановление Правительства Российской Федерации от 1 ноября 2012г. № 1119 «об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». [↑](#footnote-ref-2)
3. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [↑](#footnote-ref-3)