**Техническое задание**

Поставка и настройка программного обеспечения для системы "Предбиллинг 3-6 ЦК"для нуждАО ЭнергосбыТ Плюс

1. **Общие положения**
   1. **Назначение и область применения**

Настоящее Техническое Задание (далее – ТЗ) определяет обязательный перечень функций программного обеспечения (далее – ПО) системы «Предбиллинг 3-6 ЦК» в части сбора (опроса приборов учёта), получения/импорта, проверки, обработки, хранения, отображения и передачи/экспорта в биллинговую систему и иным лицам показаний интервальных приборов учёта электрической энергии (далее – Интервальных ПУ) клиентов АО «ЭнергосбыТ Плюс», применяемых для расчётов в группах точек поставки (далее – ГТП) с 3 – 6 ценовой категорией.

* 1. **Организационный объем**

В рамках настоящего ТЗ требуется выполнить поставку и внедрение ПО системы «Предбиллинг 3-6 ЦК», а также консультирование сотрудников в следующих регионах присутствия:

* Оренбургский филиал АО «ЭнергосбыТ Плюс»;
* Кировский филиал АО «ЭнергосбыТ Плюс»;
* Ивановский филиал АО «ЭнергосбыТ Плюс».
  1. **Сроки выполнения работ**

Работы выполняются в соответствии с Приложением №1 к настоящему ТЗ и Договору на поставку программного обеспечения и внедрение системы «Предбиллинг 3-6 ЦК» АО «ЭнергосбыТ Плюс».

* 1. **Место выполнения работ**

Работы по внедрению ПО системы «Предбиллинг 3-6 ЦК» выполняются удаленно. Перед предоставлением удаленного доступа к Инфраструктуре Заказчика Исполнитель предоставляет Чек-лист проведения оценки состояния информационной безопасности при взаимодействии с третьими лицами по форме Приложения №3 к настоящему техническому Заданию

* 1. **Общие требования к ПО**
     1. ПО должно обладать архитектурой, обеспечивающей выполнение следующих характеристик:
* комфортная работа большого количества пользователей с большими массивами справочной информации и данных энергопотребления (при условии достаточных вычислительных мощностей серверного оборудования);
* поддержка многопоточности и многозадачности функционирования серверного оборудования на базе ПО и интерфейса, в том числе возможность формирования отчётов, запросов одновременно с уже запущенными аналогичными процессами;
* Архитектурная модель и платформа ПО, а также технология разработки компонентов должны обеспечивать развитие путём добавления новых модулей и интеграции с новыми приложениями и новым оборудованием.
  + 1. Каждый компонент серверной части ИВК на базе ПО должен иметь возможность установки на выделенный сервер, включая возможность размещения обслуживающих публичные сервисы компонент в демилитаризованной зоне (DMZ). В то же время не должна быть исключена возможность консолидации двух и более произвольных компонент на одном или нескольких выделенных серверах;
    2. АРМ пользователей любой категории, представленные Веб-кабинетами, должны осуществлять подключение к серверной части с использованием сети Интранет или Интернет (в зависимости от выбранной модели доступа) и защищённого (безопасного) соединения;
    3. ПО должно обеспечивать высокую производительность в крупных территориально распределённых системах, включающих десятки тысяч точек учёта, в том числе:
* возможность распределения функций ПО определённой роли – сбор данных (опрос приборов учёта, импорт из файлов), получение/импорт, проверку (анализ качества данных), обработку, расчёты и передачу/экспорт – путём установки на серверную часть компонентов прикладного ПО, отвечающих за соответствующие функции;
* при использовании нескольких серверов – доступ к данным всей системы в прозрачном режиме без необходимости проведения процедур отложенной передачи данных (синхронизации, репликации) и дополнительных манипуляций с системой управления базой данных (далее – СУБД);
* управление серверами всех прикладных ролей (сбор, анализ, расчёты, веб-доступ);
* исключение необходимости синхронизации нормативной справочной информации между серверами и сопутствующих коллизий.
  + 1. ПО должно обеспечивать пользователям непрерывный доступ к информационным ресурсам, данным за исключением периодов времени, необходимых для проведения регламентных работ;
    2. Должна быть предусмотрена возможность работы ПО как на физических, так и на виртуализованных серверных мощностях;
    3. Система должна иметь поддержку кластеризации и балансировки нагрузки на серверной части программного комплекса;
    4. Расширение лицензии ПО должно обеспечиваться заменой ключевого файла без необходимости переустановки ПО и конвертации базы данных;
    5. ПО должно обеспечивать гибкую настройку пользовательских прав и ролей, с возможностью конфигурировать интерфейс, в зависимости от роли пользователя;
    6. Требования к производительности:
* обеспечивать эффективную работу с данными не менее 10 000 Интервальных ПУ;
* обеспечивать параллельную работу не менее 8 пользователей системы, включая 1 Администратора;
* отклик интерфейса на любые действия пользователя не должен превышать 3 сек.
  + 1. Требования к документированию:
* разработать проектную документацию на Систему[[1]](#footnote-1);
* разработать частное техническое задание и частный технический проект на подсистему обеспечения информационной безопасности Системы
* Иная проектная и эксплуатационная документация в соответствии с Приложением №1 (в составе Отчетных документов).
  1. **Требования к интерфейсу пользователя**
     1. Интерфейс пользователей ПО должен поддерживать многозадачность и возможность одновременной работы из нескольких вкладок одного Веб-браузера.
  2. **Брендирование и кастомизация интерфейса**
     1. Для соответствия фирменному стилю и интеграции с личными кабинетами потребителя ПО должно иметь возможность брендирования – настройки цветовой схемы основного интерфейса:
* настройка цветовой схемы интерфейса - основной цвет, цвета шрифта на фоне основного цвета, выделения, шрифта на фоне выделения, чередования, шрифта на фоне чередования, разделов настройки, функциональных разделов, системных разделов, кнопок управления;
* установка произвольного логотипа, отображаемого в заголовке основного экрана интерфейса ПО;
* настройка цветов и установка логотипа должны производиться в основном интерфейсе ПО. Настройка цветов должна проводиться заданием цветовых кодов HTML для каждого типа элемента интерфейса с возможностью выбора из палитры без необходимости ручной правки файлов шаблонов/стилей. Настройки должны сохраняться при обновлении версий ПО.
  1. **Поддержка системного ПО**
     1. ПО должно полноценно функционировать на различных уровнях серверной части с использованием следующего системного программного обеспечения, СУБД и поддержкой всех приведённых ниже вариантов:

серверная часть:

* Astra Linux;
* РЕД ОС.

СУБД:

* PostgreSQL (версия 9.6 и выше);
* Postgres Pro (версия 9.6 и выше).

АРМ пользователей:

* Microsoft Windows XP и старше, GNU/Linux (включая дистрибутивы Ubuntu/Runtu, openSUSE и др.);
* Microsoft Excel 2007 и старше, Adobe Reader 9 и старше, OpenOffice.org версии 3 и старше.

Поддержка ПО в серверной части ОС ALT Linux и РЕД ОС должна подтверждаться двусторонними сертификатами совместимости, заверенными компанией-разработчиком соответствующей ОС.

* + 1. В качестве браузеров для реализации веб-кабинетов всех категорий пользователей для приведённого перечня платформ в ПО должны поддерживаться следующие актуальные версии:
* Microsoft Edge;
* Google Chrome;
* Яндекс Браузер;
* Mozilla Firefox;
* Opera.

1. **Функциональные требования к системе** 
   1. **Общие требования:** 
      1. ПО должно обеспечивать опрос (чтение данных) Интервальных ПУ, приём/импорт, передачу/экспорт, проверку, обработку, хранение в БД и отображение:

* значений результатов измерений Интервальных ПУ, которые выражены в числовых значениях (кВт\*ч с учётом коэффициента измерительного комплекса или без него) с дискретностью 30 или 60 минут;
* показаний Интервальных ПУ нарастающим итогом, зафиксированных на границе суток/месяца, которые выражены в числовых значениях (кВт\*ч с учётом коэффициента измерительного комплекса или без него).

ПО должно обеспечивать прием указанных значений, которые могут поступать/направляться, в разных формах/форматах файлов/отчётов (xml или MS Excel файлах). Время загрузки в БД значений, указанных в п.2.1.1, должно быть:

* не менее 14 880 значений за 60 секунд в среднем, при импорте из xml файла;
* не менее 29 760 значений за 60 секунд в среднем, при импорте из файла MS Excel.
  1. **Требования к подсистеме НСИ**
     1. Подсистема НСИ ПО должна содержать описатель справочников и иерархические (древовидные) представления объектов системы.

Системные справочники, которые должны по умолчанию содержаться в ПО:

* абоненты, физические лица;
* абоненты, юридические лица;
* абоненты, сетевые организации;
* измерительные трансформаторы;
* приборы учёта;
* устройства сбора и передачи данных (УСПД).
  + 1. Подсистема НСИ должна содержать конструктор типов измерительных трансформаторов, приборов учёта и устройств сбора и передачи данных (УСПД) с возможностью определить соответствующие метрологические характеристики.
  1. **Иерархические представления**
     1. ПО должно содержать функцию классификации через построение иерархических представлений, которые должны позволять описывать различные элементы системы, прежде всего точек учёта (ТУ), в привязке к различным формам древовидного описания, причём:
* количество типов и количество самих иерархических представлений не должно быть ограничено, должна быть возможность создавать/редактировать новые реестры (справочники) с произвольной структурой и назначением;
* глубина формирования иерархического представления не должны быть ограничены по количеству используемых типов (классов) объектов и возможных уровней иерархии;
* правила построения иерархических представлений не должны быть жёстко зашиты в ПО, а должны гибко настраиваться.

Должны быть предусмотрены следующие системы классификации ТУ:

* коммерческий и технический учёт;
* описание топологии электрической сети, включая определение схемы питания с градацией по уровням напряжения и привязкой потребителей;
* описание географической привязки объектов учёта;
* прочие возможные системы классификации должны реализовываться настройками ПО.
* удаление/изменение параметров объекта в одном из классификаторов, должно транслироваться на тот же объект других классификаторов.
  1. **ГИС (Картография)**
     1. ПО должно обеспечивать возможность позиционирование объектов системы на географической карте с использованием подложек следующих поставщиков геоинформационных решений:
* OpenStreetMap.
  1. **Фильтрация и поиск**
     1. Подсистема НСИ должна быть готова к работе с большим количеством элементов справочников и иерархических (древовидных) представлений. Для оптимизации работы с компонентами НСИ ПО должно содержать следующие встроенные функции:
* поиск и фильтрация по одному или совокупности критериев с возможностью установки логического соответствия между критериями (по принципам И/ИЛИ/НЕ);
* группировка справочников по значениям различных полей;
* динамическая дозагрузка в интерфейс пользователя содержимого справочников и иерархических представлений по мере необходимости, функции «пейджинга», для минимизации нагрузки на каналы связи и на АРМ пользователя.
  1. **Требования к подсистеме сбора данных и взаимодействия с внешними системами**
     1. ПО должно поддерживать дистанционный опрос (чтение данных) приборов учёта и УСПД распространённых типов/производителей счётчиков электрической энергии (Интервальных ПУ), таких как – Энергомера, Инкотекс, Миртек, Милур, Системы и Технологии, Эльстер Метроника, МИР, РИМ, Прософт Системы, Landis+Gir, НЗиФ им.Фрунзе:
* обеспечивать опрос (чтение данных) приборов учёта и УСПД с использованием различных технологий связи (CSD, GPRS) в автоматическом режиме по расписанию и в ручном режиме;
* чтение из приборов учёта и УСПД текущего времени, его коррекцию/синхронизацию.
  + 1. Подсистема сбора данных должна быть оптимизирована для работы с большим количеством GSM-соединений и GPRS-сессий, оперируя консолидированным справочником SIM-карт и поддерживать функцию управления модемным пулом с групповым управлением и разделением на обслуживающих операторов сотовой связи.
    2. ПО должно иметь возможность выполнять опрос (чтение данных) приборов учёта и/или УСПД с задержкой не более одних суток, при условии работоспособности приборов учёта, оборудования сбора данных и каналов связи.
    3. ПО должно обеспечивать автоматическую синхронизацию времени на уровне ПУ и УСПД с точностью ведения времени не хуже 5,0 с в сутки, в том числе посредством источника точного времени, получающего информацию о точном времени от датчиков.
    4. Подсистема сбора данных должна обеспечить возможности:
* исключения повторного сбора из ПУ и/или УСПД ранее полученных данных;
* настройки одного основного и произвольного количества резервных маршрутов опроса (чтения) данных с указанием приоритета их использования;
* использования для определения маршрута элемента реестра (справочника) сотовых операторов и SIM-карт;
* определения в системе модемного пула, состоящего из произвольного количества модемов и комплексно используемого для организации коммутируемых соединений с ПУ или УСПД;
* опрос в ручном режиме параллельно множества ПУ или УСПД;
* предоставления пользователю обобщенной и детализированной информации о ходе выполнения сценариев опроса с её представлением в табличном и/или графическом виде.
  + 1. Настройка подсистемы сбора данных должна предусматривать:
* возможность создания сценариев сбора данных в привязке к ветви иерархии ТУ и всем входящим в неё ПУ и/или УСПД;
* возможность при добавлении в ветвь иерархии нового ПУ или УСПД от пользователя не должно требовать дополнительных требований для включения этого ПУ или УСПД в сценарий сбора данных;
* возможность определения категорий маршрутов сбора данных только для автоматических сценариев, только ручных запросов или комбинированных.
  + 1. ПО должно поддерживать:
* опрос приборов учёта по протоколу СПОДЭС (Национальный стандарт Российской Федерации ГОСТ Р 58940-2020 «Требования к протоколам обмена информации между компонентами интеллектуальной системы учета и приборами учета», утвержден приказом Росстандарта от 28.07.2020 №415), который предусмотрен приказом Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 30.12.2020 №788 «Об утверждении перечня и спецификации защищенных протоколов передачи данных, которые могут быть использованы для организации информационного обмена между компонентами интеллектуальной системы учета электрической энергии»;
* информационный обмен данными с интеллектуальными системами учета электрической энергии (мощности) с использованием протокола по спецификации ПОДИС, утверждённых приказом Минэнерго России от 30.12.2020 №1234;
* информационный обмен по открытому программному интерфейсу приложения (API), снабжённому описанием для автоматизированного обмена данными и использования функций ПО;
  + 1. ПО должно обеспечивать (при реализации 2-го этапа):
* автоматический экспорт через email, ftp, локальные и сетевые директории макетов xml 80020 (80021), 80040 (80041), различных файлов xml, xls (xlsx), txt, csv, pdf и т.д. произвольной структуры при условии разработки соответствующего шаблона экспорта;
* автоматический импорт через email, ftp, локальные и сетевые директории макетов xml 80020 (80021), 80040 (80041) различных файлов xml, xls (xlsx), txt, csv и т.д. произвольной структуры при условии разработки соответствующего шаблона импорта. При этом (не обязательное требование):
* не должны игнорироваться символы (точка, запятая) в значениях;
* должны игнорироваться значения, имеющие знак «плюс», «минус», амперсанд и т.п. Сообщение о таких значениях должно отображаться в интерфейсе загрузки;
* новые шаблоны экспорта и импорта различных файлов xml, xls (xlsx), txt, csv произвольной структуры должны иметь возможность быть реализованными без привлечения разработчика ПО и без необходимости выполнять обновление ПО;
* при импорте через email должна быть предусмотрена настройка гибкой логики адресации полученных сообщений по различным критериям, включая адрес отправителя, тему письма, тело письма, наименование файла-вложения.
  + 1. ПО должно обеспечивать (при реализации 2-го этапа):
* автоматический импорт через email, ftp, локальные и сетевые директории макетов файлов формата xml, xls (xlsx), содержащих информацию об объектах (договорах, ГТП, точках поставки и измерения (ПУ) и т.п.) на основе которых в системе должны быть созданы указанные объекты и применяемые к ним схемы расчётов (сальдо перетока/потребления).
  + 1. API должен предусматривать возможности:
* автоматических приёма и передачи описаний объектов НСИ и их атрибутов, справочников приборов учёта, каналообразующего оборудования, физических и юридических лиц, измерительных трансформаторов;
* автоматических приёма и передачи всех поддерживаемых данных учёта, событий, времени ПУ и системы
* настройки регламента и расписания автоматических приёма-передачи данных через механизм заданий информационного обмена в основном интерфейсе ПО
* шифрования трафика, передаваемого по API, авторизацию субъекта информационного обмена с парольной защитой
* при приёме данных по API – возможность автоматически создавать новые ТУ и объекты НСИ в соответствии с импортируемой информацией, при передаче данных – автоматически передавать данные по новым объектам, добавленным в ветвь иерархии, для которой организована передача НСИ.
  1. **Требования к функциям хранения данных**
     1. Хранение данных должно осуществляться в специализированной БД, находящейся под управлением одной из обязательных к поддержке СУБД.
     2. Глубина хранения данных в БД должна составлять не менее 5 лет.
     3. ПО должно обеспечивать функцию разделения данных по источникам получения для обрабатываемых ТУ (сопоставленный на целевой период времени ПУ, информационный обмен, ручной ввод и т.д.) с параллельным хранением всех массивов данных в БД. Для различных источников получения данных, в привязке к узлам системы и конкретным ТУ, должна быть предусмотрена функция установки приоритетности.
     4. Для каждого значения результатов измерения в БД должны быть определены следующие параметры:
* значения результатов измерения;
* метка времени измерения;
* метка времени занесения значения результатов измерения в БД;
* источник данных (опрос ПУ, импорт из файла, импорт из системы, ручной ввод);
* единица измерения;
* статус измерения (признак достоверности).
  + 1. ПО должно обеспечивать функции:
* поддержки реляционных СУБД;
* возможность горизонтального разделения (шардинг) БД PostgreSQL, Postgres Pro, в случае приобретения соответствующего модуля расширения серверов БД;
* периодического автоматического архивирования БД с настройкой из собственного интерфейса и возможностью указать предельное количество резервных копий;
* периодической автоматической оптимизации БД по настраиваемому расписанию с настройкой из собственного интерфейса ПО;
* ограничения глубины хранения индивидуально по различным параметрам и группам ТУ (ветвям иерархии) с расписанием автоочистки и контролем длительности очистки с настройкой из собственного интерфейса ПО.
  1. **Требования к функциям представления данных**
     1. ПО должно содержать стандартные функции представления данных за выбранный интервал времени в рамках интерфейса АРМ пользователей, включая:
* отображение данных Интервальных ПУ в ТУ в табличной и графической формах с отображением в веб-интерфейсе в виде:
* линейных графиков;
* круговых диаграмм;
* диаграмм с отображением долей потребления выбранных точек учёта от общего потребления;
* гистограмм, в т.ч. с накоплением;
* отображение журналов событий по объектам системы в табличной форме;
* отображение результатов импорта и экспорта данных;
* отображение событий приборов учёта.

Стандартные функции представления должны иметь возможность расширения с помощью функций подсистемы генерации отчётных форм.

* 1. **Требования к подсистеме аналитических функций**
     1. Подсистема аналитических функций ПО должна предусматривать следующие функции:
* визуально понятная карта в привязке к иерархическим представлениям, на которой показан процент сбора (наличия в БД) данных по каждому активному ПУ или УСПД, в составе системы, с представлением сопутствующей диагностической информации;
* визуально понятная карта в привязке к иерархическим представлениям, где показан статус наличия/отсутствия связи и собранных (имеющихся) данных ПУ или УСПД при выбранной глубине пропадания связи с представлением сопутствующей диагностической информации;
* интерфейс расчёта балансов/потребления по узлам/объектам распределительной сети/энергопринимающим устройствам, включая данные по фактическому, допустимому небалансам и уровень потерь. Функция должна быть реализована с учётом топологии сети и известных метрологических характеристик измерительных комплексов. Должен быть предусмотрен конструктор расчёта балансов/потребления, позволяющий сконфигурировать схему расчёта баланса/потребления для выбранного объекта системы;
  + 1. Подсистема (при реализации 2-го этапа) должна иметь интерфейс достоверности данных, оперирующий совокупностью алгоритмов и критериев, позволяющих оценить достоверность/качество данных (в БД) и отобразить результаты, а именно;
* разность между суммой 30 или 60 минутных значений и расходом по показаниям на границе месяца, с учётом коэффициента измерительного комплекса, измерительный канал ПУ которого участвует в расчётах в расчётном периоде. Также должны быть определены – знак и величина полученной разности, по каждому измерительному каналу ПУ, участвующему в расчётах отчетного периода. Функция должна предусматривать отображение результатов проверочного расчёта, значение которого превышает настраиваемое значение (% и/или кВт\*ч), либо их фильтрацию;
* контроль наличия/отображение отрицательных значений сальдо перетока/потребления по ГТП (каждой в отдельности), с возможностью выгрузки в редактируемый отчёт;
* отображение разницы значений сальдо перетока/потребления по ГТП (каждой в отдельности):
* в сравнении с предыдущим месяцем;
* в сравнении со средним значением за предыдущие несколько месяцев (настраиваемое значение);
* контроль наличия/отображение информации об одинаковости/равности показаний на границе месяца, измерительных каналов ПУ, участвующих в расчётах отчетного периода.
* возможность ручной модификации, ручного ввода данных, их замещения с помощью различных методик и алгоритмов.
  + 1. ПО должно производить расчёт следующих показателей:
* сальдо/потребления по ГТП/объекту;
* суммарное энергопотребление в ТУ;
* потери в силовом электрическом оборудовании, в том числе, в соответствии с Методикой расчёта потерь в редакции Приказа №326 Минэнерго РФ;
* баланс по элементам сети/системы;
* расчет «на лету» производных учетных показателей – показателей с большей дискретностью из показателей с меньшей дискретностью – объём потребления за час/сутки/месяц из значений 30-минутной энергии/мощности. Рассчитанные данные должны снабжаться соответствующим признаком и визуально выделяться в интерфейсе.
  + 1. ПО должно производить расчёт следующих значений (при реализации 2-го этапа):
* расчёт 30 или 60 минутных значений измерительного канала Интервального ПУ по его расходу (показаниям на границе месяца с учётом коэффициента измерительного комплекса) или величине недоучёта, с возможностью распределения ровным графиком или по 30 или 60 минутным значениям сальдо потребления по ГТП и применение результатов расчёта (профиля) в расчётах;
* расчёт замещающих значений для тех интервалов (30 или 60 минут) измерительного канала Интервального ПУ значения которые отсутствую частично или полностью. Замещающие значения должны иметь цветовую разметку. Функция должна давать пользователю ПО возможность выбора метода расчёта замещающей информации, а также введение произвольного значения, в том числе, массово.
  1. **Требования к подсистеме генерации отчётных форм**
     1. Подсистема генерации отчётных форм ПО должна обладать следующими характеристиками:
* должна предоставляться возможность создавать шаблоны MS Excel отчётных форм произвольной структуры и наполнения без необходимости привлечения разработчика ПО;
* конструктор отчётных форм должен быть встроен непосредственно в офисный пакет MS Excel с использованием специализированной панели инструментов;
* должна быть предусмотрена возможность установки произвольного набора входных параметров для каждого шаблона отчётной формы;
* формирование отчётных форм должно выполняться в ручном, а также в автоматическом режиме с возможной отправкой по электронной почте, сохранении в указанную директорию;
* должна быть предусмотрена возможность формирование отчётных форм в фоновом режиме, даже при выходе пользователя из системы;
* формирование отчётных форм должно быть предусмотрено в различных форматах, включая xml, MS Excel и Adobe Pdf.
  1. **Требования к подсистеме тревог**
     1. ПО должно содержать встроенную подсистему тревог, включая гибкий конструктор тревог, позволяющий определить список реакций и адресатов на каждую конкретную нештатную ситуацию.

Каждая тревога должна проходить процедуру квитирования и может быть помещена в архив только после квитирования ответственным пользователем с текстовым комментарием.

* + 1. Каналы оповещения пользователей о возникновении тревог:
* сообщение электронной почты на адрес;
* SMS-сообщение на номер;
* цветовая индикация в Веб-кабинете соответствующего пользователя;
* нотификации в мобильных платформах Google Android, выполненные по общим правилам соответствующих ОС.
  1. **Требования к подсистеме безопасности**
     1. Все Веб-серверы и Веб-приложения, входящие в комплект ПО, должны поддерживать использование сертификатов безопасности и механизмов шифрования SSL или TLS, работая в протоколе HTTPS.

Исполнитель должен обеспечивать выполнение требований по информационной безопасности для WEB –разработки в соответствии с требованиями согласно Приложению № 2 к настоящему Техническому заданию.

* + 1. В основе подсистемы безопасности ПО должна лежать ролевая модель доступа. При этом роли должны определять типовые модели функционального поведения и ограничений. Каждый пользователь может относиться к одной или нескольким ролям. Совокупность ограничений каждого пользователя должна определяться логической суммой соответствующих ролей и собственных параметров пользователя.
    2. Для ролей и пользователей должны быть доступны следующие параметры и ограничения:
* права на объекты системы, включая ТУ в привязке к иерархическим представлениям;
* права на справочники, включая установку опции управления (создание, чтение, редактирование, удаление);
* права на отчёты;
* права на использование различных разделов интерфейса пользователя, выполнение различных операций, использование различных функций системы.
  + 1. В ПО должны быть предусмотрены:
* защищённое хранилище паролей устройств;
* сквозная аутентификация пользователей с использованием ActiveDirectory без хранения паролей пользователей в ПО;
* аутентификация без ввода пароля – возможность входа для зарегистрированной учётной записи по специальному одноразовому токену в URL при переходе по ссылке;
* поддержка электронной цифровой подписи для формируемых отчётов;
* журналирования всех действий пользователей с отображением журнала с возможностью фильтрации по периодам, типам событий/действий, пользователям;
* журналирование попыток несанкционированного доступа;
* встроенная политика требований к паролям пользователей - минимальная и максимальная длина пароля, обязательность использования цифр, символов в верхнем и нижнем регистрах, запрет применения стандартных простых паролей.
  + 1. В ПО должна быть предусмотрена настраиваемая политика безопасности, включающая следующие составляющие:
* Разрешения самостоятельного и периодического изменения и сброса паролей;
* Управление длительностями и прерываниями сессий пользователей;
* Управление блокировками пользователей, автоматическая блокировка хостов и пользователей при обнаружении попыток несанкционированного доступа;
* Использование CAPTCHA для дополнительной аутентификации пользователей;
* Использование двухфакторной аутентификации пользователей через sms, e-mail, нотификации в мобильных приложениях;
* Политику групповых и индивидуальных уведомлений пользователей о событиях безопасности.
  + 1. Модель безопасности ПО должна позволять гибко настраивать зоны доступа как в общесистемном режиме, так и в режиме ИСП, в том числе с разграничением полномочий внутри конкретного ИСП.

В ходе оказания услуг Исполнитель должен выполнить работы по информационной безопасности:

* + 1. В ходе оказания услуг Исполнитель должен выполнить работы:
       1. определить уровень защищенности персональных данных (далее – ПДн) (если ИС будет обрабатывать ПДн) в соответствии с ПП-1119[[2]](#footnote-2) и присвоения категории значимости ИС в качестве объекта критической информационной инфраструктуры (далее – ОКИИ) (или обоснование отсутствия необходимости присваивать категорию значимости ИС) в соответствии с ПП-127[[3]](#footnote-3);
       2. Разработать документ Модели угроз безопасности информации в соответствии Методикой ФСТЭК[[4]](#footnote-4), если ИС обрабатывает ПДн и/или ей присвоена категория значимости;
       3. Осуществить выбор мер обеспечения безопасности информации в ИС в соответствии с Моделью угроз и определенными уровнем защищенности ПДн[[5]](#footnote-5) и присвоенной категории значимости[[6]](#footnote-6);
       4. Разработать частное техническое задание на создание подсистемы безопасности информации ИС;
       5. Разработать частный технический проект на создание подсистемы безопасности информации ИС.
       6. Отчетные документы:

- Эскизный проект;

- Акт предварительной оценки уровня защищенности ПДн,

- Акт предварительного категорирования,

- Модель угроз безопасности информации,

- Частное техническое задание на создание подсистемы безопасности информации ИС;

- Частный технический проект на создание подсистемы безопасности информации ИС;

- Протокол проведения испытаний в соответствии с проектной документацией по информационной безопасности.

2.12.7.8. На этапе реализации провести испытания в соответствии с проектной документацией.

1. **Порядок работы Исполнителя при осуществлении удаленного доступа к инфраструктуре Заказчика**

Требования к Исполнителю при осуществлении удаленного доступа к инфраструктуре.

* 1. Исполнитель предоставляет перечень IP-адресов, принадлежащих подрядчику, 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.
  12. Условия предоставления удаленного доступа
  13. Исполнитель должен предоставить чек-лист проведения оценки состояния информационной безопасности, на основании которого Заказчик оценивает возможность предоставления удаленного доступа (Приложение 3 к настоящему ТЗ). Исполнитель по запросу Заказчика должен предоставить копии (выдержки) документов, указанных в чек-листе проведения оценки состояния информационной безопасности.
  14. 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:
      1. на оборудовании должно быть установлено лицензионное общесистемное программное обеспечение, находящееся на поддержке производителя;
      2. на оборудовании должны быть установлены последние обновления для общесистемного программного обеспечения, включая обновления безопасности;
      3. 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);
      4. 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.
  15. **Требования к гарантийному обслуживанию прикладного ПО**
      1. Гарантийные обязательства должны осуществляться в течение гарантийного периода – 12 месяцев, начиная с даты подписания Акта приема-передачи прав.
      2. В течение гарантийного периода выполняются гарантийные обязательства по исправлению ошибок в ПО, включая как скрытые, так и явные ошибки ПО.
      3. Порядок обработки ошибок в ПО:
* обращение по электронной почте с подробным описанием выявленной проблемы, спецификацией используемого оборудования, прилагаемыми журналами, снимками экрана и иной информацией, позволяющей точно идентифицировать проблему;
* запрос дополнительной информации в том случае, если ранее переданной информации недостаточно для идентификации проблемы;
* определение сроков исправления ошибки ПО;
* по итогам исправления ошибки в ПО передаются все компоненты ПО (исполняемые модули, скрипты и т.д.) и документацию, затронутые данным исправлением. Исправления в части исполняемых модулей могут передаваться как в виде обновлений (патчей), так и виде обновленного дистрибутива ПО.
  1. **Требования к составу эксплуатационной документации**
     1. Программное обеспечение должно сопровождаться полным комплектом эксплуатационной документации (ЭД), в который должны входить:
* Руководство по эксплуатации для администратора.
* Руководство по эксплуатации для пользователя.
* Комплект ЭД передается в составе комплекта ПО.
* Паспорт на Систему.
  + 1. Иная проектная и эксплуатационная документация в соответствии с Приложением №1 (в составе Отчетных документов).
  1. **Требования к сроку и условиям гарантийного обслуживания**

Гарантия на поставляемое ПО должна распространяться не менее чем на 12 месяцев.

Приложение №1

к Техническому заданию на поставку программного обеспечения

для системы «Предбиллинг 3-6 ЦК»

**Календарный план график выполнения работ**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **п/п** | **Плановые сроки** | | **Наименование этапа** | **ОТЧЕТНЫЕ ДОКУМЕНТЫ** |
| **Дата**  **начала** | **Дата**  **завершения** |  |  |
| **Этап №1 - Поставка программного обеспечения** | | | |  |
| **1** |  | Не позднее 19.12.2023 | Поставка программного обеспечения, соответствующего пунктам настоящего Технического задания, за исключением п.2.6.8, п.2.6.9 п.2.9.2, п.2.9.4, 2.10.1 настоящего Технического задания | Акт на приёма –передачи неисключительного права на использование ПО (форма – Приложение №5);  Спецификация (форма - Приложение№ 4);  Руководство по эксплуатации (разворачиванию и обслуживанию ПО) для администратора (в составе комплекта ПО);  Руководство по эксплуатации для пользователя (в составе комплекта ПО). |
| **2** |  | Описание и размещение служб ПО на оборудовании Заказчика, разработка частного (детализированного) технического задания | Эскизный проект, частное (детализированное) техническое задание |
| **3** |  | Настройка работы служб ПО | Отчёт о работе служб ПО;  Протокол тестирования ПО; |
| **4** |  | Подписание отчетных документов 1 этапа | Акт сдачи- приемки выполненных работ (оказанных услуг) – по форме Приложения №3 |
| **Этап №2 – Доработка программного обеспечения (не менее 7 000 чел\*часов)** | | | |  |
| **5** |  | Не позднее 30.09.2024 | Реализация функционала п.2.6.8, п.2.6.9 п.2.9.2, п.2.9.4, 2.10.1 настоящего Технического задания | Сценарии тестирования ПО;  Протоколы функционального, интеграционного и нагрузочного тестирования;  Руководство по эксплуатации для пользователя;  Паспорт на Систему |
| **6** |  | Выполнение требований по информационной безопасности | Акт предварительной оценки уровня защищенности ПДн,  Акт предварительного категорирования,  Модель угроз безопасности информации,  Частное техническое задание на создание подсистемы безопасности информации ИС;  Частный технический проект на создание подсистемы безопасности информации ИС;  Протоколы проведения испытаний в соответствии с проектной документацией. |
| **7** |  | Проведение обучения работе в системе персонала Заказчика | Отчёт об обучении сотрудников |
| **8** |  | Подписание отчетных документов 2 Этапа | Акт сдачи –приемки выполненных работ (оказанных услуг)- по форме Приложения №3 |

Приложение № 2

к Техническому заданию на поставку программного обеспечения

для системы «Предбиллинг 3-6 ЦК»

**ТРЕБОВАНИЯ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

**для WEB разработки**

Оглавление

[1. Требования к защите от НСД 1](#_Toc102046437)

[2. Требования к сетевому взаимодействию и каналам связи 2](#_Toc102046438)

[3. Требования к защите соединений 2](#_Toc102046439)

[4. Требования к механизмам аутентификации и авторизации 2](#_Toc102046440)

[5. Требования к управлению сессиями 3](#_Toc102046441)

[6. Требования к организации ввода данных 3](#_Toc102046442)

[7. Требования к механизмам отладки и аудита 4](#_Toc102046443)

[8. Требования к реализации доступа к файловой системе 4](#_Toc102046444)

[9. Требования к загрузке и хранению пользовательских данных 4](#_Toc102046445)

[10. Требования к интеграции с корпоративными системами 4](#_Toc102046446)

[11. Требования к безопасности кода 5](#_Toc102046447)

[12. Требования к десериализации. 6](#_Toc102046448)

[13. Требования к актуальности компонентов информационной системы. 6](#_Toc102046449)

[14. Соблюдение требований законодательства и ЛНА в части конфиденциальных данных (персональные данные, коммерческая, служебная тайна и прочее). 6](#_Toc102046450)

1. **Требования к защите от НСД**
   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. Протоколы аудита системы и приложений должны быть защищены от несанкционированного доступа как локально, так и в архиве.
  2. Система должна предотвратить работу с некатегоризированной информацией под сеансом пользователя, авторизованного на доступ к конфиденциальной информации.
  3. Система должна обеспечивать разделение полномочий администраторов и персонала, обеспечивающего ее функционирование, возможность назначения минимально необходимых прав и полномочий.

1. **Требования к сетевому взаимодействию и каналам связи**
   1. Защищённая часть системы должна быть отделена от незащищённой части системы межсетевым экраном.
   2. Данные, передаваемые по сети, шифруются с использованием TLS. Безопасный канал используется для всех сервисов приложения.
   3. Настройки TLS соответствуют современным лучшим практикам, или максимально приближены к ним, если операционная система не поддерживает рекомендуемые стандарты.
   4. Приложение верифицирует X.509 сертификаты сервера во время установления защищённого канала. Принимаются только сертификаты, подписанные доверенным удостоверяющим центром (CA).
   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.
   6. Приложение не полагается на единственный небезопасный канал связи (e-mail или SMS) для таких критических операций, как регистрация и восстановление аккаунта.
   7. Приложение использует только актуальные версии библиотек для подключения к сети и обеспечения безопасного соединения.

**3. Требования к защите соединений**

* 1. Все клиент-серверные взаимодействия должны осуществляться с использованием защищенного транспортного протокола через TLS версии не ниже 1.2.
  2. Для принудительного использования HTTPS для всех запросов необходимо использовать strict-transport-security (HSTS) заголовки.
  3. Используемые Cookie должны быть httponly и ограничены путем и доменом.
  4. Для веб-приложений необходимо использовать Content Security Policy, разрешающую минимально необходимый перечень источников контента.
     1. **Требования к механизмам аутентификации и авторизации**
  5. Все интерактивные формы HTML должны быть защищены от Cross-Site Request Forgery (CSRF).
  6. 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.
  7. 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.
  8. Использовать при восстановлении пароля эффективные методы восстановления учётных данных и паролей.
  9. Пароли и другие аутентификационные данные не должны содержаться в исходном коде.
  10. Пароли и другие аутентификационные данные должны передаваться только через шифрованные и аутентифицированные протоколы.
  11. Пароли должны обрабатываться необратимыми хэш-функциями при их вводе. Запрещено оперировать паролями в незащищенном виде.
  12. Аутентификационные и авторизационные данные не должны передаваться на сторону клиента. Это гарантирует невозможность компрометации путем манипуляций программным обеспечением на стороне клиента.
  13. Пароли и другие конфиденциальные данные, такие как Session IDs и Database IDs, никогда не должны передаваться как URL-параметр в HTTP Get запросах.
  14. Пароль никогда не должен показываться в открытом виде (при вводе и других формах).
  15. 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).
  16. 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.
  17. Аутентификационные данные должны храниться в зашифрованном виде.
  18. Максимальная длина пароля и количество типов используемых символов не должны быть ограничены.
  19. 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).
  20. При изменении конфиденциальных данных рекомендуется инициировать повторный процесс аутентификации пользователя.

1. **Требования к управлению сессиями**
   1. Продолжительность сессии пользователя должна быть ограничена (ограничение по времени бездействия пользователя).
   2. Механизм установления сессий (Session Management) должен быть защищен от атак на перехват сессии (Session Fixation attacks).
   3. Длина идентификатора сессии должна быть не менее 128 бит. Идентификатор сессии должен быть абстрактным относительно функционала ПО.
   4. Должна соблюдаться высокая степень энтропии нумерации сессий, рекомендуется использовать метод случайных чисел.
   5. Недопустимо передавать идентификатор сессии как часть URL. Рекомендуется использовать параметризированные HTTPS запросы или Cookie.
   6. Должен обеспечиваться сбор, запись и хранение информации о действиях персонала и администраторов.
2. **Требования к организации ввода данных**
   1. Вводимые в приложение данные должны подвергаться синтаксической и семантической проверкам, вводимые пользователем данные проверяются, фильтруются и очищаются.
   2. Должны использоваться надежные механизмы экранирования при передаче вводимых пользователем данных для предотвращения SQL-инъекций. Аналогичный подход необходимо использовать при передаче файлов.
   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.
   4. Должен проверяться синтаксис выводимых данных на предмет отсутствия спецсимволов для предотвращения XSS-атак
   5. Необходимо использовать безопасный API, исключающий применение интерпретатора или предоставляющий параметризованный интерфейс, либо использовать инструменты объектно-реляционного отображения (ORM).
   6. Взаимодействие с приложением по интерфейсу API рекомендуется ограничить доступ по белому списку IP-адресов или иных источников подключения.
   7. Все общедоступные формы ввода данных должны быть защищены от множественной отправки с помощью капчи.
   8. Все приватные формы должны быть защищены от множественной отправки с помощью rate-limit.
3. **Требования к механизмам отладки и аудита**
   1. Сообщения об ошибках не должны содержать конфиденциальной информации, такой как данные пользователя, stack traces, dumps, данные логов и прочее.
   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.
   3. В информационной системе необходимо использовать контроль целостности журналов аудита важных транзакций для предотвращения подмены или удаления данных.
   4. В информационной системе необходимо регистрировать сбои и уведомлять администраторов при необходимости (например, если сбои повторяются).
4. **Требования к реализации доступа к файловой системе**
   1. Для доступа к файловой системе должны использоваться нормализованные и приведенные к корню разрешенного каталога пути.
   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.
5. **Требования к загрузке и хранению пользовательских данных**
   1. При загрузке определенных типов файлов, должны выполняться проверки их типа и/или расширения.
   2. Должны быть реализованы проверки загрузки файлов только в разрешенные каталоги.
   3. Объемы загрузки данных должны быть лимитированы минимально необходимыми.
   4. Хранилища критичных данных должны шифроваться, в том числе резервные копии.
   5. Кэширование ответов, содержащих конфиденциальные данные, должно быть отключено.
6. **Требования к интеграции с корпоративными системами**

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.

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

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

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

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

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.

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

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

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

При выборе алгоритма шифрования необходимо руководствоваться требованиями законодательства РФ.

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

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

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

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

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.

1. **Требования к безопасности кода**
   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.
  1. 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.
  + 1. **Требования к десериализации.**
  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.
    1. **Требования к актуальности компонентов информационной системы.**
  1. На все компоненты информационной системы должны быть установлены обновления безопасности.
  2. Рекомендуется выполнять регулярное обновление компонентов информационной системы не реже одного раза в 3 месяца.
  3. Обновления должны устанавливаться только из доверенных источников (с официальных сайтов и репозиториев производителей программного обеспечения).
     1. **Соблюдение требований законодательства и ЛНА в части конфиденциальных данных (персональные данные, коммерческая, служебная тайна и прочее).**
  4. 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.
  5. 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 субподрядчики 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 на поставку программного обеспечения

для системы «Предбиллинг 3-6 ЦК»

**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 подрядчиком 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. При разработке технических решений и формировании всей проектной документации следует придерживаться подходов, описанных в национальных стандартах:

   - ГОСТ Р 59793-2021 Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания.

   - ГОСТ 34.602-2020 Информационные технологии. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы.

   - ГОСТ 34.201-2020 Информационные технологии. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем. [↑](#footnote-ref-1)
2. ПП-1119 – Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». [↑](#footnote-ref-2)
3. ПП-127 – Постановление Правительства РФ от 08.02.2018 № 127 «Об утверждении правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей значимости объектов критической информационной инфраструктуры Российской Федерации и их значении». [↑](#footnote-ref-3)
4. Методика ФСТЭК – Методический документ «Методика оценки угроз безопасности информации», утвержденный ФСТЭК России 05.02.2021. [↑](#footnote-ref-4)
5. В соответствии с Приказом 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-5)
6. В соответствии с Приказом ФСТЭК России от 25.12.2017 № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» [↑](#footnote-ref-6)