Список работ и дополнительные требования

Наименование работ/услуг
1 Предпроектное исследование и планирование: • Проведение анализа существующей ИТ-инфраструктуры Заказчика, включая оценку аппаратного и программного обеспечения, сетевой архитектуры и политик безопасности. • Разработка и согласование детальной схемы внедрения, определяющей последовательность работ, точки интеграции и критерии успешности. • Формирование и согласование с Заказчиком исчерпывающего перечня проводимых работ (Scope of Work). • Разработка и согласование Программы и Методики Испытаний (ПМИ), определяющей процедуры проверки функциональности и соответствия требованиям. **2 Развертывание и настройка КриптоПро CSP 5.0:** • Подготовка стандартизированного пакета установки (MSI) с предварительно настроенными параметрами и необходимыми компонентами. • Разработка и применение групповых политик (GPO) для централизованной установки, активации и первоначальной настройки ПО на целевых рабочих станциях. • Пилотное развертывание на 3 эталонных ПК: проверка работы электронной подписи в целевых приложениях, импорт и настройка доверенных корневых сертификатов, конфигурация политик проверки ЭП. • Организованное поэтапное развертывание на оставшиеся рабочие станции (52 шт.) партиями по 10 единиц с контролем установки и пост-установочной проверкой функциональности. **3 Тестирование, демонстрация и завершение проекта:** • Проведение приемо-сдаточных испытаний в соответствии с утвержденной ПМИ. • Тестирование всех функций развернутого решения, выявление, диагностика и устранение возможных неисправностей или несоответствий. • Проведение демонстрации работоспособности системы Заказчику, подтверждение выполнения всех согласованных требований. • Формирование итогового отчета по проекту, включающего описание выполненных работ, результаты испытаний и рекомендации по эксплуатации.

4 Развертывание и конфигурация средств защиты информации:
• Установка и первичная настройка 8 экземпляров средства анализа защищенности «Сканер ВС»
версии 7.
• Установка, базовая настройка и ввод в эксплуатацию сервера управления средствами защиты
информации Secret Net Studio версии 8.x.
• Установка и настройка клиентской части Secret Net Studio версии 8.x на 55 целевых рабочих станциях
пользователей, включая интеграцию с сервером управления и настройку политик безопасности.

5 Подготовка анкет и анализ предоставленной информации о информационной системе, для подключения
к сети "Вуз онлайн" (далее – ИС), включая:
• анализ размещения объекта и определение границ контролируемой зоны (далее - КЗ);
• анализ размещения линий и коммуникаций объектов;
• анализ состояния охраны и пропускного режима;
• анализ организации охранной и пожарной сигнализации;
• анализ (уточнение) перечня сведений, подлежащих защите;
• анализ перечня и объема обрабатываемых данных, определение границ ИС;
• анализ информационных характеристик и организационных структур ИС;
• анализ условий расположения ИС относительно границ КЗ;
• анализ конфигураций и топологий ИС и систем связи в целом и их отдельных компонентов,
физические, функциональные и технологические связи как внутри этих систем, так и с другими
системами различного уровня и назначения;
• анализ технических средств и систем, предполагаемых к использованию в ИС и системах связи,
условия их расположения, общесистемные и прикладные программные средства, применяемые в
обследуемой системе и предлагаемые к использованию;
• анализ технологического процесса обработки информации;
• анализ режимов обработки информации в ИС в целом и в отдельных компонентах;
• анализ степени участия персонала в обработке (обсуждении, передаче, хранении) информации,
характер их взаимодействия между собой;
• анализ распределения ответственности должностных лиц за выполнение требований по обеспечению
защиты информации и уровня их подготовки;
• анализ существующей организационно-распорядительной и методической документации.

6 Разработка Модели угроз безопасности информации для ИС, которая включает в себя построение «Модели нарушителя» и определение

актуального типа угроз.
Классификация ИС на основании уровня значимости информации и масштаба ИС. Составление «Акта классификации».

7 Разработка Требований по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных в соответствии с требуемым уровнем защищенности
ИСПДн и Моделью угроз безопасности информации.

8 Разработка перечня рекомендаций (организационных и технических мер) по приведению информационной системы персональных данных в соответствие Требованиям по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных.

9 Разработка организационно-распорядительной документации, необходимой при обработке персональных данных (далее - ПДн) в организации:
• Положение о постоянно действующей экспертной комиссии по информационной безопасности.
• Политика в отношении обработки ПДн.
• Положение о порядке обработки и защиты ПДн субъектов ПДн.
• Положение по технической защите информации.
• Инструкция ответственного за организацию работ по обработке ПДн.
• Инструкция администратора безопасности информации.
• Инструкция пользователя ИСПДн.
• План мероприятий по информационной безопасности.
• Перечень обрабатываемых ПДн.
• Перечень ИСПДн.
• Перечень должностей, которым доступ к ПДн, обрабатываемым в ИСПДн и без использования средств
автоматизации, необходим для выполнения трудовых обязанностей.
• Форма перечня помещений, в которых ведётся обработка ПДн.
• Форма перечня мест хранения ПДн.
• Перечень разрешённого программного обеспечения.
• Перечень событий безопасности.
• Состав постоянно действующей комиссии по информационной безопасности.
• Регламент реагирования на запросы и обращения субъектов ПДн и их представителей,
уполномоченного органа по защите ПДн.
• Журнал учёта запросов и обращений субъектов персональных данных и их представителей.
• Журнал ознакомления и обучения сотрудников, непосредственно осуществляющих обработку ПДн.
• Журнал учета машинных носителей персональных данных.
• Журнал резервного копирования.
• Акт оценки вреда при обработке ПДн.

• Форма списка доступа (матрица доступа).
• Форма акта уничтожения ПДн.
• Форма уведомления о факте обработки ПДн.
• Форма уведомления об отказе подтверждения факта обработки ПДн.
• Форма уведомления о внесении изменений в ПДн.
• Форма уведомления об отказе внесения изменений в ПДн.
• Форма уведомления об уничтожении ПДн.
• Форма уведомления об отказе в уничтожении или прекращении обработки ПДн.
• Форма согласия субъекта ПДн и его представителя на обработку ПДн.
• Форма обязательства о неразглашении ПДн.
• Форма уведомления о трансграничной передаче.
• Форма уведомления об инциденте, заключающемся в неправомерной или случайной передаче
(предоставлении, распространении, доступе) персональных данных, повлекшей нарушение прав
субъектов персональных данных
• Форма поручения на обработку.
В случае необходимости применения средств криптографической защиты информации (далее - СКЗИ)
дополнительно осуществляется разработка следующей документации:
• Инструкция об организации и обеспечении безопасности хранения, обработки и передачи информации
по каналам связи с использованием СКЗИ.
• Инструкция администратора информационной безопасности при работе с СКЗИ.
• Инструкция пользователя СКЗИ.
• Инструкция по действиям при нештатных ситуациях.
• Порядок разрешительного доступа пользователей и эксплуатирующего персонала к
автоматизированным рабочим местам (далее - АРМ) с установленными СКЗИ.
• Журнал учёта СКЗИ, эксплуатационной и технической документации к ним.
• Журнал инструктажа персонала.
• Журнал учёта хранилищ.
• Журнал учёта мероприятий по контролю организации работ с СКЗИ.
• Технический (аппаратный) журнал.
• Форма перечня лиц, допущенных к самостоятельной работе с СКЗИ.
• Форма акта установки и ввода в эксплуатацию СКЗИ.
Форма типового акта об уничтожении криптографических ключей, содержащихся на ключевых носителях,
и ключевых документов.

10 Оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных:
• Составление программы и методик проведения оценки эффективности.

• Проведение испытаний в рамках программы и методик (оценка полноты организационно-распорядительной документации, оценки физической защиты, испытания технических средств защиты информации). Оформление протокола испытаний и заключения по результатам испытаний.

Работы по установке и настройке средств защиты информации и оценки эффективности реализованных мер по обеспечению безопасности персональных данных выполняются для 55 рабочих мест, расположенных по адресу г.Новосибирск, пр-т Карла Маркса, 26.

Работы по установке и настройке средств защиты согласно выполняются очно на площадке заказчика (выполнение отдельных видов работ возможно только после согласования с заказчиком).

Изменения в составе работ возможны только после согласования с заказчиком.