Отчёт слушателя курса ТЗКИ:	Кравченко Руслан Викторович

Тема:	**6.4. Разработка аналитического обоснования необходимости создания системы защиты информации на объекте информатизации**
Вид занятия:	Практическое занятие
Срок предоставления отчёта:	**Выложить в СДО**

Негосударственное образовательное учреждение
дополнительного профессионального образования
«Институт информационных технологий «АйТи»

Информационная безопасность. Техническая защита конфиденциальной информации

(Тема 6.4. Разработка аналитического обоснования необходимости создания системы защиты информации на объекте информатизации)

Практикум

Описание информационной системы персональных данных организации ИСПДн «Кадры»

Организация: ЗАО «Солнышко».
Директор: Иванов Иван Иванович.
Заместитель директора: Петрова Тамара Васильевна.
Главный конструктор: Старков Игорь Анатольевич
Руководитель службы: безопасности Жарков Петр Петрович
Начальник отдела ИБ: Семенов Семен Семенович.
Начальник отдела кадров: Южина Мария Ивановна.
Сотрудники отдела кадров: Сидорова Александра Павловна,
Копылова Юлия Фёдоровна.
Руководитель предпроектного обследования: Краснов Иван Иванович

Описание ИСПДн:

Состав:

1. Персональные данные сотрудников организации:
   - фамилия, имя, отчество
   - дата и место рождения
   - пол
   - сведения об образовании
   - сведения о предыдущем месте работы
   - семейное положение (ФИО жены/мужа, ФИО и даты рождения детей)
   - адреса регистрации и фактического проживания
   - номера контактных телефонов
   - индивидуальный номер налогоплательщика
   - номер страхового свидетельства пенсионного страхования
   - номер полиса обязательного медицинского страхования
   - данные водительского удостоверения

В информационной системе одновременно обрабатываются данные 777 субъектов персональных данных (сотрудников) в пределах Организации.

2. Три автоматизированных рабочих места (АРМ) пользователей, сетевой принтер, сервер, коммутационное оборудование.

Топология: АРМ и сервер составляют сегмент корпоративной вычислительной сети (см. схему).

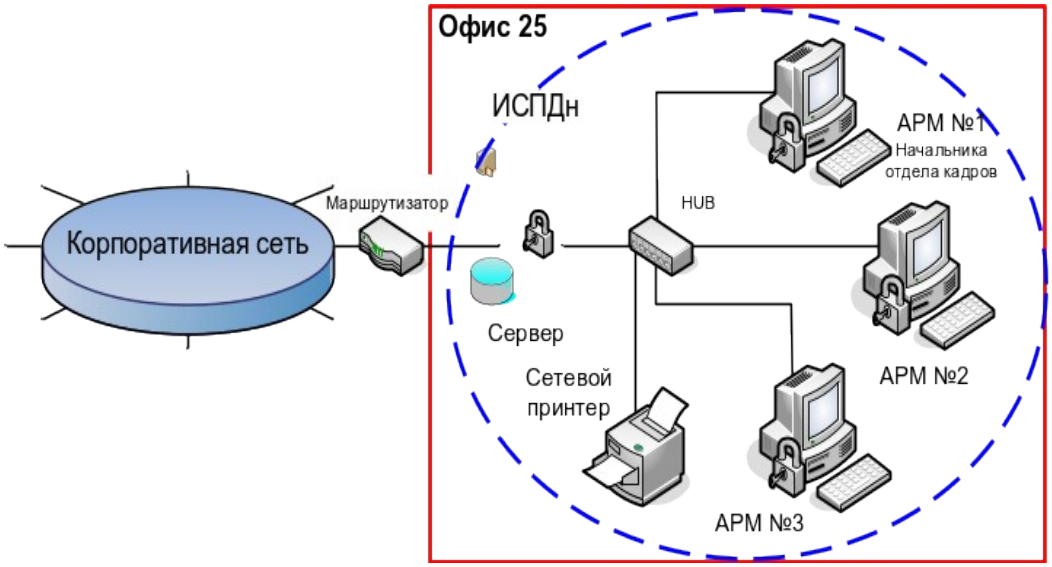

Схема ИСПД «Кадры» ЗАО «Солнышко»

Корпоративная сеть Организации не имеет подключение к сетям связи общего пользования и сетям международного информационного обмена.

В состав каждого АРМ входят два жёстких диска, на первом установлена операционная система, прикладное программное обеспечение и общедоступная справочная информация, на втором - информация, составляющая персональные данные сотрудников Организации.

1. Комплект АРМ №1-3 (см. схему): Системный блок № XXXXXXX01-03, Монитор Samsung N710 – серийный номер YYYYYYY01-03, клавиатура Genius серийный номер ZZZZZZZZ01-03, графический манипулятор (мышь) Genius серийный номер WWWW01-03.

Состав ПО для обработки ПД:

1. Клиентская часть ПО «1С:Зарплата и кадры государственного учреждения 8» хранит информацию о сотрудниках, кандидатах и соискателях (в версии КОРП) в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (https://v8.1c.ru/statehrm/dlya-kadrovoy-sluzhby/).

2. Диспетчер печати.

2. В состав сервера входят три жестких диска, на первом установлена операционная система, прикладное программное обеспечение, второй и третий объединены в RAID массив, в котором хранится информация, составляющая персональные данные сотрудников Организации.

Комплект сервера: Системный блок № XXXXXXX04, Монитор Samsung N710 – серийный номер YYYYYYY04, клавиатура Genius серийный номер ZZZZZZZZ04, графический манипулятор Genius серийный номер WWWW04.

Состав ПО для обработки ПД:
1. Серверная часть ПО «1С:Зарплата и кадры государственного учреждения 8» хранит информацию о сотрудниках, кандидатах и соискателях (в версии КОРП) в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (https://v8.1c.ru/statehrm/dlya-kadrovoy-sluzhby/).
2. Диспетчер печати.

Сервер и коммуникационное оборудование установлены в типовой стойке.

Сетевой принтер HP LaserJet P2015 серийный номер SSSSSSSSS.

Коммутатор: Коммутатор Cisco WS-C2960CX-8TC-L.

Маршрутизатор: Маршрутизатор Cisco Small Business RV340-K8-RU.

3. Технология обработки персональных данных:

Обработка персональных данных сотрудников включает весь перечень действий.

К работе на АРМ допущены сотрудники отдела кадров и заместитель директора.

Полный доступ ко всей информации на АРМ и сервере имеют заместитель директора и начальник отдела кадров.

Сотрудники отдела кадров имеют полный доступ только к каталогу «Личные дела», размещённой на диске №2 своего АРМ, и только на чтение информации из каталога «Личные дела» на сервере.

Системный администратор сегмента сети не имеет доступа к информации, составляющей персональные данные. Имеет права на инсталляцию, настройку программного обеспечения, программных (программно-аппаратных) средств защиты сервера и АРМ № 1-3.

Режим работы - одновременный.

Расположение: Отдельный кабинет по адресу: РФ, г. Глухов, ул. Кривая, дом 6, офис 25. Помещение офиса оборудовано охранной сигнализацией и в нерабочее время сдается под охрану. Доступ в помещение ограничен распорядительными актами Организации и автоматизированной системой контроля и управления доступа.

УТВЕРЖДАЮ[1]

_____

(должность руководителя организации)

_____

(подпись)

«_____» _____ 202 ____г.

Аналитическое обоснование необходимости создания системы защиты информации на объекте информатизации ИСПДн «Кадры»

_____

(наименование ИСПДн)

СОГЛАСОВАНО

_____

«____» _____ 202___ г.

СОГЛАСОВАНО

_____

«____» _____ 202___ г.

202_ г.

[1] Аналитическое обоснование подписывается руководителем предпроектного обследования, согласовывается с главным конструктором (должностным лицом, обеспечивающим научно-техническое руководство создания объекта информатизации), руководителем службы безопасности и утверждается руководителем предприятия-заказчика. Перечень сведений конфиденциального характера составляется заказчиком объекта информатизации и утверждается его руководителем.

Содержание

1. Термины и определения

1. Автоматизированное рабочее место – программно-технический комплекс, предназначенный для автоматизированной деятельности определенного вида.

2. Администратор автоматизированной системы – лицо, ответственное за функционирование автоматизированной информационной системы в установленном штатном режиме работы.

3. Администратор защиты (безопасности) информации – лицо, ответственное за защиту автоматизированной информационной системы от несанкционированного доступа к информации.

4. Аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора.

5. Безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

6. Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

7. Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

8. Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

9. Вспомогательные технические средства и системы – технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персональных данных.

10. Доступ к информации – возможность получения информации и ее использования.

11. Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

12. Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

13. Использование персональных данных – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

14. Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

15. Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

16. Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

17. Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

18. Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

19. Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

20. Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

21. Обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

22. Общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

23. Объект защиты информации - информация, или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с поставленной целью защиты информации.

24. Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, организующее и (или) осуществляющее обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

25. Перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

26. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

27. Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

28. Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

29. Раскрытие персональных данных – умышленное или случайное нарушение конфиденциальности персональных данных.

30. Распространение персональных данных – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

31. Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

32. Система – совокупность взаимосвязанных и взаимодействующих элементов.

33. Средства защиты информации – технические, программные средства, вещества и (или) материал, предназначенные или используемые для защиты информации.

34. Средства криптографической защиты информации – аппаратные, программные и программно-аппаратные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и

предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении.

35. Специальные категории персональных данных – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни субъекта персональных данных.

36. Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

37. Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

38. Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п

39. Угроза безопасности информации – совокупность условий и факторов, создающих потенциальную или реальную существующую опасность, связанную с утечкой информации и/или непреднамеренными воздействиями на нее.

40. Учетная запись пользователя – набор данных, однозначно идентифицирующих пользователя в системе, совокупность прав и привилегий доступа к объектам и набор квот системных ресурсов.

41. Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

42. Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

43. Уязвимость – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

44. Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность

информации в условиях случайного и/или преднамеренного искажения (разрушения).

2. Принятые сокращения

АВС	–	антивирусные средства
АРМ	–	автоматизированное рабочее место
АС	–	автоматизированная система
ГИС	–	государственная информационная система
ГОСТ	–	государственный стандарт
ИБ	–	информационная безопасность
ИС	–	информационная система, обрабатывающая информацию
КЗ	–	контролируемая зона
ИТ	–	информационные технологии
ЛВС	–	локальная вычислительная сеть
НДВ	–	не декларированные возможности
НЖМД	–	накопитель на жестких магнитных дисках
НСД	–	несанкционированный доступ
ОЗУ	–	оперативное запоминающее устройство
ОПО	–	общесистемное программное обеспечение
ОС	–	операционная система
ОТСС	–	основные технические средства и системы
ПДн	–	персональные данные
ПК	–	программный комплекс
ПО	–	программное обеспечение
ПС	–	программные средства
ПТС	–	программно-технические средства
ПЭВМ	–	персональная электронно-вычислительная машина
РД	–	руководящий документ
СВТ	–	средства вычислительной техники
СЗИ	–	система защиты информации
СКЗИ	–	средства криптографической защиты информации
СПО	–	специальное программное обеспечение
СрЗИ	–	средства защиты информации
ТЗ	–	техническое задание
ТС	–	технические средства
ТП	–	технический проект
ФСБ	–	Федеральная служба безопасности
ФСТЭК	–	Федеральная служба технического и экспортного контроля

3. Общие положения

Необходимостью создания ТЗКИ в ИСПД «Кадры» ЗАО «Солнышко» является обеспечение защиты информации при ее обработке в информационной системе.

СЗИ представляет собой совокупность организационных и технических мер, направленных на предотвращение неправомерного или случайного доступа к защищаемой информации, уничтожения, изменения, блокирования, копирования, распространения, а также иных неправомерных действий с ней.

Система защиты информации должна:

защищать ИС от вмешательства посторонних лиц в процесс её функционирования (возможность использования ИС и доступ к её ресурсам должны иметь только зарегистрированные установленным порядком пользователи);

предоставлять доступ конкретным пользователям ИС только к тем ресурсам ИС, к которым он необходим для выполнения своих служебных обязанностей, то есть защищать от несанкционированного доступа: к информации, обрабатываемой в ИС, средствам вычислительной техники, аппаратным и программным средствам защиты;

регистрировать действия пользователей при использовании защищаемых ресурсов ИС в системных журналах и анализировать содержимое этих журналов с целью контроля корректности действий пользователей;

контролировать целостность среды исполнения программ и ее восстановление в случае нарушения;

защищать от несанкционированной модификации и контролировать целостность программных средств, а также обеспечить защищу системы от внедрения несанкционированных программ;

защищать информацию, хранимую, обрабатываемую и передаваемую по каналам связи, от несанкционированного разглашения или искажения;

своевременно выявлять источники угроз безопасности информации, причины и условия, способствующие их появлению, создавать механизмы оперативного реагирования на угрозы;

создавать условия для минимизации наносимого ущерба неправомерными действиями физических и юридических лиц, уменьшать негативное влияние и ликвидировать последствия нарушения безопасности информации.

Для аналитического обоснования необходимости создания СЗИ использовалась Модель угроз безопасности информации для ИСПДн ЗАО «Солнышко»», разработанная на основании следующих документов:

ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию;

«Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденная Заместителем директора ФСТЭК России 15 февраля 2008 г;

«Методика оценки угроз безопасности информации», утвержденная Заместителем директора ФСТЭК России 5 февраля 2021 г.

Для разработки модели угроз безопасности информации на договорной основе была привлечена организация - ФГУП «НПП «Бэтта», аккредитованная ФСТЭК России в качестве органа по аттестации объектов информатизации (Аттестат аккредитации органа по аттестации №СЗИ RU.082/2.В29.274, Лицензия по ТЗКИ - регистрационный №0019 от 31 октября 2002г), совместно с начальником отдела по информационной безопасности (ИБ) ЗАО «Солнышко».

4. Описание систем и сетей и их характеристика как объектов защиты[2]

Угрозы для ИСПДн «Кадры» ЗАО «Солнышко» обусловлены преднамеренными или непреднамеренными действиями физических лиц, или организаций (в том числе террористических), а также криминальных группировок, создающими условия (предпосылки) для нарушения безопасности персональных данных (ПДн), которые ведут к ущербу жизненно важным интересам личности, общества и государства.
ИСПДн «Кадры» ЗАО «Солнышко» представлена в виде:

Персональные данные сотрудников организации:

- фамилия, имя, отчество
- дата и место рождения
- пол
- сведения об образовании
- сведения о предыдущем месте работы

---

[2] Для описания п.4-7 используйте материалы Модели угроз ПДн, разработанные на ПЗ 4.1.

На предпроектной стадии по обследованию объекта информатизации:

устанавливается необходимость обработки (обсуждения) конфиденциальной информации на данном объекте информатизации;

определяется перечень сведений конфиденциального характера, подлежащих защите от утечки по техническим каналам;

определяются (уточняются) угрозы безопасности информации и модель вероятного нарушителя применительно к конкретным условиям функционирования;

определяются условия расположения объектов информатизации относительно границ КЗ;

определяются конфигурация и топология ИСПДн и систем связи в целом и их отдельных компонент, физические, функциональные и технологические связи как внутри этих систем, так и с другими системами различного уровня и назначения;

определяются технические средства и системы, предполагаемые к использованию в разрабатываемой ИС и системах связи, условия их расположения, общесистемные и прикладные программные средства, имеющиеся на рынке и предлагаемые к разработке;

определяются режимы обработки информации в ИС в целом и в отдельных компонентах;

определяется класс защищенности ИСПДн;

определяется степень участия персонала в обработке (обсуждении, передаче, хранении) информации, характер их взаимодействия между собой и со службой безопасности;

определяются мероприятия по обеспечению конфиденциальности информации в процессе проектирования объекта информатизации.

- семейное положение (ФИО жены/мужа, ФИО и даты рождения детей)
- адреса регистрации и фактического проживания
- номера контактных телефонов
- индивидуальный номер налогоплательщика
- номер страхового свидетельства пенсионного страхования
- номер полиса обязательного медицинского страхования
- данные водительского удостоверения

В информационной системе одновременно обрабатываются данные 863 субъектов персональных данных (сотрудников) в пределах Организации.

4.1 Архитектура и схема подключений информационной системы
ИСПДн «Кадры» ЗАО «Солнышко» представлена в виде:

Три автоматизированных рабочих места (АРМ) пользователей, сетевой принтер, сервер, коммутационное оборудование.

Топология: АРМ и сервер составляют сегмент корпоративной вычислительной сети (см. схему).

Схема ИСПД «Кадры» ЗАО «Солнышко»

Для передачи информации в ИСПДн «Кадры» ЗАО «Солнышко» используется ЛВС, расположенная по адресу:
РФ, г. Глухов, ул. Кривая, дом 6, офис 25.

В процессе обработки персональных данных участвуют:

В состав каждого АРМ входят два жёстких диска, на первом уста-новлена операционная система, прикладное программное обеспечение и общедоступная справочная информация, на втором - информация, составляющая персональные данные сотрудников Организации.
1. Комплект АРМ №1-3 (см. схему): Системный блок № XXXXXXX01-03, Монитор Samsung N710 – серийный номер YYYYYYY01-03, клавиатура Genius серийный номер ZZZZZZZZ01-03, графический манипулятор (мышь) Genius серийный номер WWWW01-03.

2. В состав сервера входят три жестких диска, на первом установлена операционная система, прикладное программное обеспечение, второй и третий объединены в RAID массив, в котором хранится информация, составляющая персональные данные сотрудников Организации.
Комплект сервера: Системный блок № XXXXXXX04, Монитор Sam-sung N710 – серийный номер YYYYYYY04, клавиатура Genius серийный номер ZZZZZZZZ04, графический манипулятор Genius серийный номер WWWW04.
Сервер и коммуникационное оборудование установлены в типовой стойке.
Сетевой принтер HP LaserJet P2015 серийный номер SSSSSSSSS.
Коммутатор: Коммутатор Cisco WS-C2960CX-8TC-L.
Маршрутизатор: Маршрутизатор Cisco Small Business RV340-K8-RU.

4.2 Описание процессов передачи информации

Обработка персональных данных в ИСПДн «Кадры» ЗАО «Солнышко» ведётся:

К работе на АРМ допущены сотрудники отдела кадров и заместитель директора.

Полный доступ ко всей информации на АРМ и сервере имеют заместитель директора и начальник отдела кадров.

Сотрудники отдела кадров имеют полный доступ только к каталогу «Личные дела», размещённой на диске №2 своего АРМ, и только на чтение информации из каталога «Личные дела» на сервере.

Системный администратор сегмента сети не имеет доступа к информации, составляющей персональные данные. Имеет права на инсталляцию, настройку программного обеспечения, программных (программно-аппаратных) средств защиты сервера и АРМ № 1-3.

Режим работы - одновременный.

4.3 Перечень программных средств, используемых для обработки персональных данных в ИСПДн «Кадры» ЗАО «Солнышко»

Обработка персональных данных в ИСПДн «Кадры» ЗАО «Солнышко» ведётся в специализированном программном обеспечении:

Состав ПО для обработки ПД:

1. Клиентская часть ПО «1С:Зарплата и кадры государственного учреждения 8» хранит информацию о сотрудниках, кандидатах и соискателях (в версии КОРП) в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (https://v8.1c.ru/statehrm/dlya-kadrovoy-sluzhby/).

2. Диспетчер печати.

Состав ПО для обработки ПД:

1. Серверная часть ПО «1С:Зарплата и кадры государственного учреждения 8» хранит информацию о сотрудниках, кандидатах и соискателях (в версии КОРП) в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (https://v8.1c.ru/statehrm/dlya-kadrovoy-sluzhby/).

2. Диспетчер печати.

Перечень имеющихся программных средств, используемых для обработки персональных данных приведены в таблице 1.

Таблица 1 – Перечень имеющихся программных средств (ПС), используемых для обработки персональных данных ИСПДн «Кадры» ЗАО «Солнышко».

№ п/п	**Наименование ПС (ее составной части)**	**Расположение объекта**	**Технология обработки (АРМ, ЛВС, Распр)**	**Субъекты ПДн**	**Объем обрабатываемых Пдн (количество записей субъектов Пдн в базе данных ИСПДн)**	**Описание режима работы с базой данных**
1	«1С:Зарплата и кадры государственного учреждения 8»	Клиентская часть	АРМ	сотрудники отдела кадров и заместитель директора	777	Одновременно
2	«1С:Зарплата и кадры государственного учреждения 8»	Серверная часть	АРМ	сотрудники отдела кадров и заместитель директора	777	Одновременно

4.4 Перечень структурных подразделений работающих с БД ИСПДн «Кадры» ЗАО «Солнышко»

Перечень структурных подразделений работающих с БД ИСПДн «Кадры» ЗАО «Солнышко» отображен в таблице 2.

Таблица 2 - Перечень структурных подразделений, работающих с БД ПДн «Кадры» ЗАО «Солнышко»

№ п/п	**Наименование БД (ее составной части)**	**Расположение объекта**	**Структурное подразделение**
1	«Личные дела»	Сервер	Отдел кадров

2	«Личные дела»	диске №2 своего АРМ	Отдел кадров

4.5 Анализ организационных мер защиты ИСПДн

В ходе проведения проверки наличия и полноты методической и организационно-распорядительной документации прямо или косвенно относящейся к защите персональных данных было установлено, что документы по данной тематике не разрабатывались.

В зданиях, где находятся помещения ИСПДн «Кадры» ЗАО «Солнышко», все двери помещений оборудованы врезными замками. Доступ в помещения, где расположены рабочие станции, ограничен, войти могут только сотрудники.

Пожарная и охранная сигнализация установлена во всех помещениях, где обрабатываются персональные данные. Охрана объекта осуществляется частным охранным предприятием на договорной основе.

4.6 Анализ технологического процесса обработки информации, реализованного в информационной системе

Согласно представленному «Технологическому процессу обработки ин-формации…» ИСПДн предназначена для обработки информации ограниченного доступа, формирования электронных документов (ЭД) и вывода их на печать. При этом информация в ИСПДн может поступать из других подразделений и организаций на учтенных бумажных или электронных носителях информации.

Для осуществления технологического процесса обработки информации в ИСПДн используется программное обеспечение (ПО), перечисленное в таблице №2.

ИСПДн «Кадры» ЗАО «Солнышко» предназначена для работы в одновременном режиме, доступ исполнителей к работе осуществляется по утвержденному списку, пользователи имеют ораничение права доступа к информации, ИСПДн не имеет подключения к сетям связи общего пользования и сетям международного информационного обмена.

Настройку систем защиты для конкретных пользователей и контроль ее работы осуществляет администратор безопасности информации. Функции, права, обязанности и порядок работы в ИСПДн администратора безопас-

ности информации и пользователей регламентируются специально разработанными инструкциями администратору безопасности информации и пользователям.

Уровень подготовки администратора безопасности и пользователей позволяет выполнять возложенные на них обязанности.

4.7Результаты классификации ИСПДн «Кадры» ЗАО «Солнышко»

В соответствии с требованиями Постановления Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», выявлено, что тип актуальных угроз безопасности персональных данным ЗАО «Солнышко» относится к **угрозам _3_ типа** – угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

В соответствии с требованиями Приказа ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» проведена классификация по уровням защищенности персональных данных при их обработке в ИСПДн «Кадры» ЗАО «Солнышко», таблица 3.

Таблица 3

№ п\п	Характеристика	Значение
1	Категория персональных данных	3
2	Субъекты ПДн	работники
3	Объем обрабатываемых ПДн	Менее 100 тыс.
4	Количество рабочих станций, входящих в состав ИСПДн	3
5	Структура ИСПДн	АРМ
6	Количество пользователей, допущенных к работе в ИСПДн	3
7	Режим обработки ПДн в ИСПДн	Многопользовательская ИСПДн с разными правами доступа
8	Разграничению прав доступа пользователей[7]	С разграничением
9	Подключение ИСПДн к локальным (распределенным) сетям общего пользования	Имеется
10	Тип ИСПДн	Типовая
11	Местонахождение технических средств ИСПДн	Внутри КЗ
12	Тип актуальных угроз (на основании разработанной модели угроз и анализа актуальных угроз в ИСПДн)	3

По результатам анализа исходных данных информационной системы персональных данных, анализа актуальности угроз безопасности в разработанной модели угроз ИСПДн «Кадры» ЗАО «Солнышко» присвоен **3 уровень защищенности**.

5. Возможные негативные последствия от реализации (возникновения) угроз безопасности информации

К основным негативным последствиям от реализации угроз безопасности ПД в ИСПДн «Кадры» ЗАО «Солнышко» определены в таблице 4.

Таблица 4

№ п/п	Виды риска (ущерба)	Актуальность	Возможные типовые негативные последствия
У1	Ущерб физическому лицу	Возможны	Угроза жизни или здоровью.
			Унижение достоинства личности.
			Нарушение свободы, личной неприкосновенности.
			Нарушение неприкосновенности частной жизни.
			Нарушение личной, семейной тайны, утрата чести и доброго имени.
			Нарушение тайны переписки, телефонных переговоров, иных сообщений.
			Нарушение иных прав и свобод гражданина, закрепленных в Конституции Российской Федерации и федеральных законах.
			Финансовый, иной материальный ущерб физическому лицу.

			Нарушение конфиденциальности (утечка) персональных данных.
			Нарушение конфиденциальности (утечка) персональных данных.
			"Травля" гражданина в сети "Интернет".
			Разглашение персональных данных граждан
У2	Риски юридическому лицу, индивидуальному предпринимателю, связанные с хозяйственной деятельностью	Возможны	Нарушение законодательства Российской Федерации.
			Потеря (хищение) денежных средств.
			Недополучение ожидаемой (прогнозируемой) прибыли.
			Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций.
			Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств).
			Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса.
			Срыв запланированной сделки

			с партнером.
			Необходимость дополнительных (незапланированных) затрат на восстановление деятельности.

Другие виды последствий также могут быть, но как правило они несут на несколько порядков меньший ущерб.

6. Возможные объекты воздействия угроз безопасности информации

Негативные последствия, объекты воздействия, виды воздействия на них в ИСПДн «Кадры» ЗАО «Солнышко» изображены в таблице 5.

Таблица 5

Негативные последствия	**Объекты воздействия**	**Виды воздействия**
Разглашение персональных данных граждан (У1)	База данных информационной системы, содержащая идентификационную информацию граждан	Утечка идентификационной информации граждан из базы данных
	Удаленное автоматизированное рабочее место (АРМ) пользователя	Утечка идентификационной информации граждан с АРМ пользователя
	Линия связи между сервером основного центра обработки данных и сервером резервного центра обработки данных	Перехват информации, содержащей идентификационную информацию граждан, передаваемой по линиям связи
	Веб-приложение информационной системы, обрабатывающей идентификационную информацию граждан	Несанкционированный доступ к идентификационной информации граждан, содержащейся в веб-приложении информационной системы

7. Источники угроз безопасности информации

Возможные цели реализации угроз безопасности ПД в ИСПДн «Кадры» ЗАО «Солнышко» нарушителями представлены в таблице 6.

Таблица 6

№ вида	Виды нарушителя	Категории нарушителя	Возможные цели реализации угроз безопасности информации
1	Преступные группы (криминальные структуры)	Внешний	Получение финансовой или иной материальной выгоды.
			Желание самореализации (подтверждение статуса)
2	Авторизованные пользователи систем и сетей	Внутренний	Получение финансовой или иной материальной выгоды.
			Любопытство или желание самореализации (подтверждение статуса).
			Месть за ранее совершенные действия.
			Непреднамеренные, неосторожные или неквалифицированные действия

Уровни возможностей нарушителей по реализации угроз безопасности ПД в ИСПДн «Кадры» ЗАО «Солнышко» представлена в таблице 7.

Таблица 7

№ п/п	Уровень возможностей нарушителей	Возможности нарушителей по реализации угроз безопасности информации	Виды нарушителей
1	Нарушитель, обладающий базовыми возможностями	Имеет возможность при реализации угроз безопасности информации использовать только известные уязвимости, скрипты и инструменты.	Физическое лицо (хакер)
		Имеет возможность использовать средства реализации угроз (инструменты), свободно	Лица, обеспечивающие поставку программных, программно-

		распространяемые в сети "Интернет" и разработанные другими лицами, имеет минимальные знания механизмов их функционирования, доставки и выполнения вредоносного программного обеспечения, эксплойтов.	аппаратных средств, обеспечивающих систем
		Обладает базовыми компьютерными знаниями и навыками на уровне пользователя.	Лица, обеспечивающие функционирование систем и сетей или обеспечивающих систем (администрация, охрана, уборщики и т.д.)
		Имеет возможность реализации угроз за счет физических воздействий на технические средства обработки и хранения информации, линий связи и обеспечивающие системы систем и сетей при наличии физического доступа к ним.	Имеет возможность реализации угроз за счет физических воздействий на технические средства обработки и хранения информации, линий связи и обеспечивающие системы систем и сетей при наличии физического доступа к ним.
		Таким образом, нарушители с базовыми возможностями имеют возможность реализовывать только известные угрозы, направленные на известные (документированные) уязвимости, с использованием общедоступных инструментов	Бывшие работники (пользователи)

8. Способы реализации (возникновения) угроз безопасности информации

Исходя из объектов воздействия и доступных интерфейсов, для каждого вида нарушителя определены актуальные способы реализации угроз безопасности ПД в ИСПДн «Кадры» ЗАО «Солнышко» представлена в таблице 8.

Примеры определения актуальных способов реализации угроз безопасности информации и соответствующие им виды нарушителей и их возможности

Таблица 8

№ п/п	**Вид нарушителя**	**Категория нарушителя**	**Объект воздействия**	**Доступные интерфейсы**	**Способы реализации**
1	Разработчики программных, программно-аппаратных средств	Внешний	ПО	Удаленное подключение	внедрение дополнительных функциональных возможностей в программные или программно-аппаратные средства

9. Актуальные угрозы безопасности информации

Из общего состава техник и тактик, приведенных в Методике оценки угроз безопасности информации: методический документ, утвержден ФСТЭК России от 5 февраля 2021 г., исключаем те, которые не связаны с используемыми у нас технологиями, не применимы к нашим процессам, не приводящие к ущербу или недоступные актуальным нарушителям. Все актуальные сценарии должны быть подмножествами их этого ограниченного набора тактик.
Перечень основных тактик и соответствующих им типовых техник, используемых для построения сценариев реализации угроз безопасности ПД в ИСПДн «Кадры» ЗАО «Солнышко» представлена в таблице 9.

Таблица 9 – Расшифровка актуальных техник и тактик реализации УБИ

№ п/	**Тактика**	**Основные техники**

п		
1	Сбор информации о системах и сетях	Т1.1. Сбор информации из публичных источников: официальный сайт (сайты) организации, СМИ, социальные сети, фотобанки, сайты поставщиков и вендоров, материалы конференций
		Т1.3. Пассивный сбор (прослушивание) информации о подключенных к сети устройствах с целью идентификации сетевых служб, типов и версий ПО этих служб и в некоторых случаях - идентификационной информации пользователей
2	Получение первоначального доступа к компонентам систем и сетей	Т2.1. Использование внешних сервисов организации в сетях публичного доступа (Интернет) Примеры: 1) доступ к веб-серверу, расположенному в сети организации; 2) доступ к интерфейсу электронной почты OutlookWebAccess (OWA) почтового сервера организации

Далее уже исходя из этих применимых тактик, возможностей нарушителей, объектов воздействия и их интерфейсов и способов реализации определены актуальные угрозы (табл.10).

Таблица 10

Группа актуальных угроз	**Уровень возможностей нарушителей**	**Объекты воздействий**	**Способы реализации**	**Негативные последствия**
Угрозы	Н2	Прикладное	С1,С10,С12	П2.2

несанкционированной модификации защищаемой информации		программное обеспечение, Платежная\ финансовая информация		
Угрозы внесения несанкционированных изменений в прикладное программное обеспечение	Н2	Прикладное программное обеспечение.	С1,С2,С10	П2.2
Угрозы сбора информации защищаемой системы	Н2	АРМ клиента ФО, ПО клиентской части VPN или драйвера СКЗИ, Каналы связи, Системное программное обеспечение, Прикладное программное обеспечение	С1,С10,С12	П2.2
Угрозы ошибочных действий	Н2	Прикладное программное обеспечение	С9	П2.2

10. ТСЗИ предлагаемые для использования ИСПДн

Для того, чтобы обеспечить ИБ организационных мер и встроенных средств недостаточно, следовательно, необходимо использовать дополнительные СЗИ формирующие подсистемы СЗИ.

Все СЗИ должны организовывать полноценную систему ЗИ и ПДн, обеспечивая полноценную защиту для конкретной ИСПДн.

Для реализации Комплексной системы ЗИ предлагается использовать сертифицированные средства ФСТЭК:

- средство защиты от НСД Dallas Lock 8.0-K;
- АПКШ «Континент» 3.7

- СЗИ "Континент WAF" IPC-1000 (S021)
- средство анализа защищенности XSpider 7.8.24
- Антивирус Kaspersky Security для бизнеса (на момент написания, данное средство уже настроено и установлено)

11. Обоснование необходимости привлечения специальных организаций

В учреждении отсутствуют необходимое контрольно-измерительное оборудование. У учреждения нет лицензий на деятельность по защите конфиденциальной информации.

В связи с большим объемом работ монтажных и пуско-наладочных, приемо-сдаточных и контрольных испытаний целесообразно привлечение сотрудников специализированной организации, имеющей лицензии на деятельность по технической защите персональных данных.

12. Оценка материальных, трудовых и финансовых затрат на разработку и внедрение ТСЗИ

Ориентировочная стоимость предлагаемых к использованию сертифицированных средств защиты информации представлена в таблице 11.

Таблица 11 Ориентировочная стоимость предлагаемых технических средств

№ п/п	**Продукт**	**Примерная стоимость, руб**
1	Средство защиты от несанкционированного доступа на 3 рабочих места	71 000,0
2	Средство анализа защищенности	23 500,0
3	Средство межсетевого экранирования и криптографической защиты	89 500,0
	ИТОГО, руб.	184 000,0

К установке и настройке средств защиты информации могут привлекаться специалисты по защиты информации оператора, разработчики информационной системы и специалисты сторонних организаций, специализирующихся на защиты информации. Расчет стоимости работ по установке СЗИ приведен в таблице 12

Таблица 12 – затраты работа на установку и настройки СрЗИ

№ п/п	**Продукт**	**Примерная стоимость, руб**
1	Установка и настройка средств защиты от несанкционированного доступа на 3 рабочих места 1 сервер	5 000,0
2	Установка и настройка средства анализа защищенности	5 000,0
3	Установка и настройка средства межсетевого экранирования и криптографической защиты	10 000,0
ИТОГО, руб.		20 000,0

Затраты на установку и настройку средств защиты информации специалистами.

К установке и настройке средств защиты информации могут привлекаться специалисты по защиты информации оператора, разработчики информационной системы и специалисты организации, специализирующихся на защиты информации.

Проведение испытаний системы защиты ИСПДн сопровождается выдачей документа, подтверждающего соответствие принятых мер защиты в соответствии с классом ИСПДн.

Проведение работ по оценке соответствия требованиям руководящих документов по защите ПДн в ИСПДн может проводить организация, имеющая лицензию на право проведения работ по защиты конфиденциальной информации. Стоимость работ приведена в таблице 12.

Таблица 12 – Перечень работ по аттестации информационной систем

Продукт	**Кол-во**	**Цена розничная, 1 шт., руб.**	**Общая стоимость, руб.**
Предварительное обследование ИСПДн (изучение технологического процесса обработки и хранения	1	20 000,0	20 000,0

защищаемой информации, анализ информационных потоков, определение состава использованных для обработки персональных данных средств)			
Анализ исходных данных, необходимых для изучения и анализа циркулирующей информации.	1	10 000,0	10 000,0
Анализ организационной структуры ИС и условий ее эксплуатации, фиксация состава технических средств, входящих в аттестуемый объект, системы ЗИ на объекте, разработанной документации и её соответствия требованиям нормативной документации по ЗИ.	1	10 000,0	10 000,0
Разработка программы и методик аттестационных испытаний	1	15 000,0	15 000,0
Проверка состояния организации работ и выполнения организационно-технических требований по защите информации, оценка правильности классификации ИСПДн, оценка уровня разработки организационно-распорядительной, проектной и эксплуатационной документации, оценка уровня подготовки кадров и распределения ответственности за выполнение требований по обеспечению безопасности информации в ИСПДн.	1	20 000,0	20 000,0
Комплексные испытания на соответствие требованиям по защите от несанкционированного доступа (НСД) к информации, обрабатываемой в ИСПДн (за 1 АРМ)	3	2 500,0	7 500,0
Контрольные испытания ИСПДн на соответствие требованиям по защите информации от несанкционированного доступа в соответствии с определенным классом защищенности от НСД для межсетевого обмена	3	1 500,0	4 500,0
Подготовка отчетной документации (протоколы испытания и заключения по результатам аттестационных испытаний, аттестат соответствия	1	20 000,0	20 000,00
ИТОГО, руб.			137 000,00

13. Ориентировочные сроки разработки и внедрения ТСЗИ

Предпроектная стадия – разработка технического (частного технического) задания на создание системы защиты ИСПДн в течение десяти дней.

Стадия проектирования – разработка проектов, включающая разработку технического проекта СЗИ в составе ИСПДн в течение двадцати дней.

Стадия ввода в действие СЗИ – включает установку, настройку, опытную эксплуатацию и приемо-сдаточные испытания средств защиты информации, а также аттестацию объекта информатизации на соответствие требованиям безопасности информации в течение тридцати дней

14. Перечень мероприятий по обеспечению конфиденциальности информации на стадии проектирования объекта информатизации

1) Организация работ по созданию и эксплуатации объектов информатизации и их системы защиты информации определены в разрабатываемом «Положении о порядке организации и проведении работ по защите конфиденциальной информации» или в приложении «К руководству по защите информации от утечки по техническим каналам на объекте» и должна предусматривать:

- Порядок определения защищаемой информации;
- Порядок привлечения подразделений организации, специализированных сторонних организаций, разработки и эксплуатации объектов информатизации и системы защиты информации, их задачи и функции на различных стадиях создания и эксплуатации объекта информатизации;
- Порядок взаимодействия всех занятых в этой работе организаций подразделений и специалистов;
- Порядок разработки ввода в действие и эксплуатацию объектов информатизации;
- Ответственность должностных лиц за своевременность и качество формирования требований по защите информации, а качество и научно-технический уровень разработки системы защиты информации.

2) Выполняемые работы на предпроектной стадии по обследованию объекта информатизации

На предпроектной стадии по обследованию объекта информатизации выполняются следующие мероприятия:

- Установление необходимости обработки (обсуждения) конфиденциальной информации на данном объекте информатизации;
- Определяется перечень сведений конфиденциального характера подлежащих защите;
- Определяются (уточняются) угрозы безопасности информации и модель вероятного нарушителя применительно к конкретным условиям функционирования объекта;
- Определяются условия расположения объекта информатизации относительно границ контролируемой зоны;
- Определяются конфигурация и топология автоматизированной системы 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;
- Определяются технические средства и системы, предполагаемые к использованию в разработанной автоматизированной системе и в системах связи, темные и прикладные программы средств, имеющиеся на рынке и предполагаемые к разработке;
- Определяются режимы обработки информации в автоматизированных системах в целом и в отдельных компонентах;
- Определяется класс защищенности в автоматизированной системе;
- Определяется степень участия персонала в обработке (обсуждении, передачи, хранении) информации, характер их взаимодействия между собой и со службой безопасности;
- Определяются мероприятия по обеспечению конфиденциальности информации на этапе проектирования объекта информатизации.

3) Содержание аналитического обоснования необходимости создания системы защиты информации

По результатам предпроектного обследования разрабатывается аналитическое обоснование необходимости создания системы защиты информации.

На основе действующих нормативно-методических документов по технической защите конфиденциальной информации с учетом

установленного класса защищенности автоматизированной системы задаются конкретные требования по защите информации, включаемые в техническое (частное техническое) задание на разработку системы защиты информации.

Предпроектное обследование в части касающейся определения защищаемой информации должно базироваться на документально оформленного перечня сведений конфиденциального характера составленного заказчиком объекта информатизации и утверждается руководителями организации-заказчика.

Аналитическое обоснование необходимости создания системы защиты информации должно содержать:

- Информационную характеристику и организационную структуру объекта информатизации;
- Характеристику комплекса основных и вспомогательных технических средств, программное обеспечение, режимов работы, технологического процесса обработки информации;
- Возможные каналы утечки информации и перечень мероприятий по их устранению и ограничению;
- Перечень предлагаемых к использованию сертифицированных средств защиты информации;
- Обоснование необходимости привлечения специализированных организаций, имеющие необходимые лицензии на право проведения работ по защите информации;
- Оценку материальных, трудовых и финансовых затрат на разработку и внедрение системы защиты информации;
- Перечень мероприятий по обеспечению конфиденциальности информации на стадии проектирования объекта информатизации.

4) Содержание технического задания на разработку системы защиты информации

Техническое (частное техническое) задание на разработку системы защиты информации должно содержать:

- Обоснование разработки;
- Исходные данные создаваемого (модернизируемого) объекта информатизации в техническом, программном, информационном и организационном аспектах;
- Класс защищенности автоматизированных систем;

- Ссылку на нормативно-методические документы, с учетом которых будет разрабатываться система защиты информации и приниматься в эксплуатацию объект информатизации;
- Требования к системе защиты информации на основе нормативно-методических документов и установленного класса защищенности автоматизированной системы;
- Перечень предполагаемых к использованию сертифицированных средств защиты информации;
- Обоснование проведения разработок собственных средств защиты информации, невозможности или нецелесообразности использования имеющихся на рынке сертифицированных средств защиты информации;
- Состав, содержание и сроки проведения работ по этапам разработки и внедрения;
- Перечень подрядных организаций-исполнителей видов работ;
- Перечень предъявляемый заказчику научно-технической продукции и документации.

5) Содержание работ на стадии проектирования и создания объекта информатизации и системы защиты информации в его составе

На стадии проектирования и создания объекта информации и системы защиты информации в его составе на основе предъявленных требований и заданных заказчиком ограничении на финансовые, материальные, трудовые и временные ресурсы осуществляются следующими мероприятиями:

- Разработку задания и проекта на строительные, строительно-монтажные работы (реконструкцию) объекта информатизации с учетом требований технического задания на разработку системы защиты информации;
- Разработку раздела технического проекта на объект информатизации в части защиты информации;
- Строительно-монтажные работы в соответствии с проектной документацией, утвержденной заказчиком, размещением и монтажом технических средств и систем;
- Разработку организационно-технических мероприятий по защите информации в соответствии с предъявленными требованиями;

- Закупка сертифицированных образцов и серийно выпускаемых в защищенном исполнении технических средств обработки, передачи и хранения информации либо их сертификации;
- Закупка сертифицированных технических средств защиты информации программных и программно-технических средств защиты информации и их установка;
- Разработка, доработка или закупка и последующая сертификация по требованиям безопасности информации, программных средств защиты информации в случае, когда на рынке отсутствует требуемые сертифицированные программные средства;
- Организация охраны и физической защиты помещений объекта информатизации, исключая несанкционированный доступ к техническим средствам обработки, ранения и передачи информации, их хищение и нарушение работоспособности, хищение носителей информации;
- Разработка и реализация разрешительной системы доступа пользователей и эксплуатации персонала к обрабатываемой (обсуждаемой) на объекте информатизированной информации;
- Выполнение инсталляции пакета прикладных программ в комплексе с программными средствами;
- Разработка эксплуатации документации на объект информатизации и средства защиты информации, а также организационно-распорядительной документации по защите информации (приказы, инструкции и другие документы);

Выполнение других мероприятий специфичных для конкретных объектов информатизации и направлений защиты информации.

Руководитель предпроектного обследования Кравченко Руслан Викторович