Отчёт слушателя курса ТЗКИ0722:	Сенотрусова Екатерина Анатольевна

Тема:	**4.1 Разработка модели угроз безопасности информации**
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 4.1. Практикум)

Москва 2023

Описание информационной системы персональных данных организации ИСПДн «Кадры»

Организация: ЗАО «Солнышко».

Директор: Иванов Иван Иванович.

Заместитель директора: Петрова Тамара Васильевна.

Начальник отдела ИБ: Семенов Семен Семенович.

Начальник отдела кадров: Южина Мария Ивановна.

Сотрудники отдела кадров: Сидорова Александра Павловна,
Копылова Юлия Фёдоровна.

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).

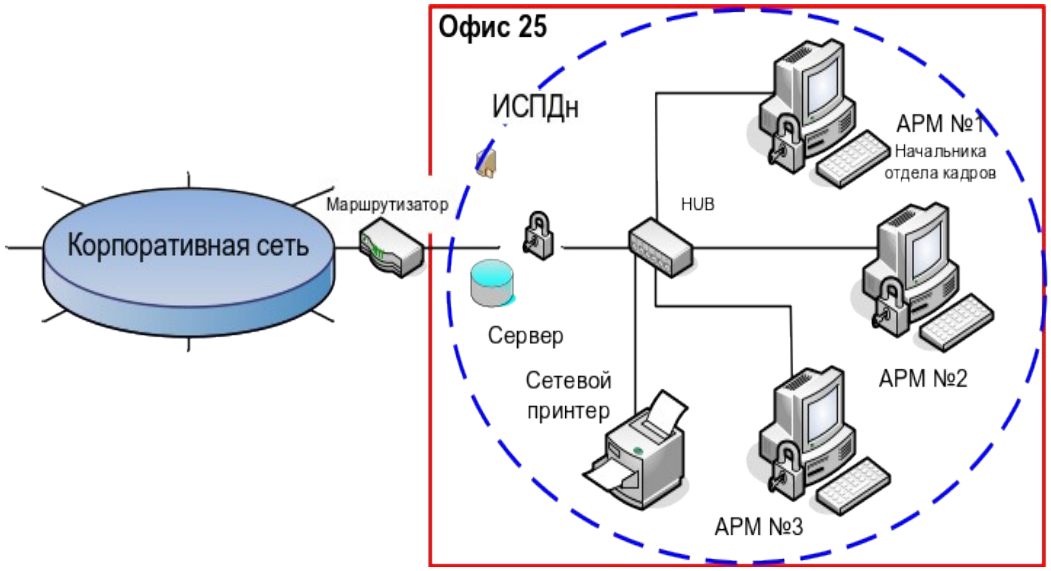

Схема ИСПД «Кадры» ЗАО «Солнышко»

Корпоративная сеть Организации не имеет подключения 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

_____

(должность руководителя организации)

_____

(подпись)

«_____» _____ 201 ____г.

Модель угроз безопасности информации
ИСПДн

_____

(наименование ИСПДн)

СОГЛАСОВАНО

_____

«____» _____ 202___ г.

СОГЛАСОВАНО

_____

«____» _____ 202___ г.

2023 г.

Содержание

1. Общие положения

Модель угроз безопасности информации для ИСПДн ЗАО «Солнышко»» разработана 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.B29.274, Лицензия по ТЗКИ - регистрационный №0019 от 31 октября 2002г), совместно с начальником отдела по информационной безопасности (ИБ) ЗАО «Солнышко».

2. Описание систем и сетей и их характеристика как объектов защиты

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:

(описание состава ИСПДн)

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.

2.1 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

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

(описание состава оборудования, технологии обработки ПД сотрудников на АРМ пользователей сегмента корпоративной сети)

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.

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.

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.

Схема ИСПДн «Кадры» ЗАО «Солнышко» представлена на рисунке 1.

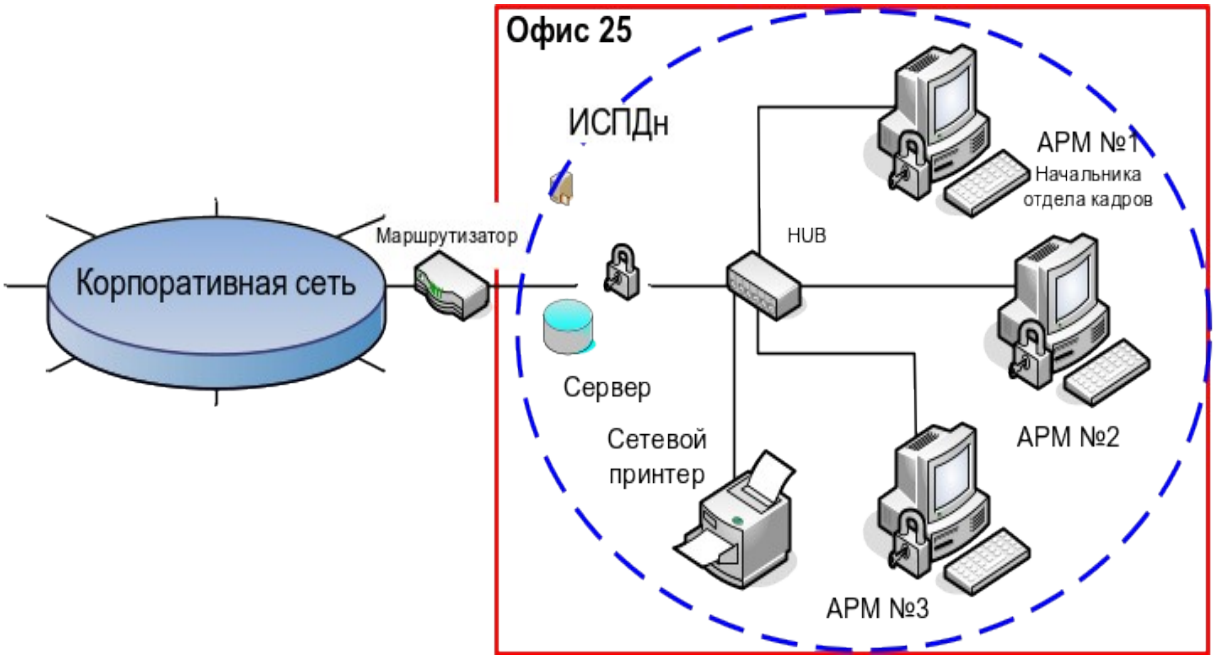

Рисунок 1 – Схема ИСПД «Кадры» ЗАО «Солнышко»

2.2 Описание процессов передачи информации.

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

(описание состава оборудования, технологии обработки ПД сотрудников на АРМ пользователей сегмента корпоративной сети)

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.

2.3 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:_____

(описание состава специализированного ПО)

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	2	3	4	9	10	11
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

2.4 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	2	3	4
1	«Личные дела»	Сервер	Отдел кадров
2	«Личные дела»	диске №2 своего АРМ	Отдел кадров

2.5 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.

2.6 Анализ технологического процесса обработки информации, реализованного в информационной системе

Согласно представленному «Технологическому процессу обработки информации…» 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 ограничение права доступа к информации, ИСПДн не имеет (имеет, 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 безопасности информации и пользователей регламентируются специально разработанными инструкциями администратору безопасности информации и пользователям.

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

2.7. Результаты 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**[1] – 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

[1] Согласно Постановлению Правительства РФ №1119 для ИСПДн различают угрозы трех типов:
Угрозы 1 типа - связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.
Угрозы 2 типа - связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.
Угрозы 3 типа - не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.
Согласно руководящему документу «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля недекларированных возможностей» (Гостехкомиссия России, 1999), **недекларированные возможности** – это функциональные возможности программного обеспечения, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

по уровням защищенности персональных данных при их обработке в ИСПДн «Кадры» ЗАО «Солнышко», таблица 3.

Таблица 3

№	Характеристика	Значение
1	Категория персональных данных[2]	3
2	Субъекты ПДн[3]	работники
3	Объем обрабатываемых ПДн[4]	Менее 100 тыс.
4	Количество рабочих станций, входящих в состав ИСПДн	3
5	Структура ИСПДн[5]	АРМ
6	Количество пользователей, допущенных к работе в ИСПДн	3
7	Режим обработки ПДн в ИСПДн[6]	Многопользовательская ИСПДн с

[2] Категории обрабатываемых персональных данных (ПДн), подразделяются на 4 группы:

1 группа — **специальные категории ПДн**, к которым относятся информация о национальной и расовой принадлежности субъекта, о религиозных, философских либо политических убеждениях, информацию о здоровье и интимной жизни субъекта;

2 группа — **биометрические ПДн**, то есть данные, характеризующие биологические или физиологические особенности субъекта и используемые для установления личности, например, фотография или отпечатки пальцев;

3 группа — **общедоступные ПДн**, то есть сведения о субъекте, полный и неограниченный доступ к которым предоставлен самим субъектом;

4 группа — **иные категории ПДн**, не представленные в трех предыдущих группах.

[3] По форме отношений между вашей организацией и субъектами обработка подразделяется на 2 вида:

- обработка персональных данных работников (субъектов, с которыми ваша организация связана трудовыми отношениями);
- обработка персональных данных субъектов, не являющихся работниками вашей организации.

[4] По количеству субъектов, ПДн которых обрабатываются, нормативным актом определены лишь 2 категории:

- менее 100 000 субъектов;
- более 100 000 субъектов;

[5] Автоматизированное рабочее место/Локальная ИСПДн / Распределенная ИСПДн

[6] Однопользовательская ИСПДн / многопользовательская ИСПДн с равными правами доступа/ многопользовательская ИСПДн с разными правами доступа

		разными правами доступа
8	Разграничению прав доступа пользователей[7]	С разграничением прав доступа
9	Подключение ИСПДн к локальным (распределенным) сетям общего пользования[8]	Имеется
10	Тип ИСПДн[9]	Типовая
11	Местонахождение технических средств ИСПДн	Внутри КЗ
12	Тип актуальных угроз[10] (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**[11]

[7] С разграничением прав доступа или без разграничения прав доступа

[8] Имеется / не имеется

[9] Типовая / специальная

[10] Типы актуальных угроз:

угрозы 1-го типа связанны с наличием недекларированных (недокументированных) возможностей в системном ПО, используемом в ИСПДн;

угрозы 2-го типа связанны с наличием недекларированных возможностей в прикладном ПО, используемом в ИСПДн;

угрозы 3-го типа не связаны с наличием недекларированных возможностей в программном обеспечении, используемом в ИСПДн.

[11] Установив исходные данные, для конкретной ИСПДн определяется уровень защищенности персональных данных в соответствии со следующей таблицей:

Таблица уровней защищенности персональных данных

Категории ПДн		Специальные			Биомет-рические	Иные			Общедоступные		
Собственные работники		нет	нет	да		нет	нет	да	нет	нет	да
Количество субъектов		более 100 тыс.	менее 100 тыс.			более 100 тыс.	менее 100 тыс.		более 100 тыс.	менее 100 тыс.	
Тип актуальных угроз	1	1 УЗ	1 УЗ	1 УЗ	1 УЗ	1 УЗ	2 УЗ	2 УЗ	2 УЗ	2 УЗ	2 УЗ
	2	1 УЗ	2 УЗ	2 УЗ	2 УЗ	2 УЗ	3 УЗ	3 УЗ	2 УЗ	3 УЗ	3 УЗ
	3	2 УЗ	3 УЗ	3 УЗ	3 УЗ	3 УЗ	4 УЗ	4 УЗ	4 УЗ	4 УЗ	4 УЗ

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

К основным негативным последствиям от реализации угроз[12] безопасности ПД в ИСПДн «Кадры» ЗАО «Солнышко» определены _____ (таблица 4).

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

Таблица 4

№	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. "Травля" гражданина в сети "Интернет". Разглашение персональных данных граждан

[12] Для определения Виды рисков (ущерба) и типовых негативных последствий от реализации угроз безопасности информации необходимо пользоваться Приложением 4 Методического документа ФСТЭК России: Методика оценки угроз безопасности информации: методический документ, утвержден ФСТЭК России 5 февраля 2021 г. – М.: 2021. – 83 с. – Текст : электронный // Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и подготовленные проекты документов по технической защите информации online. – URL: https://fstec.ru/component/attachments/download/2919.

У2	Ущерб 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.

4. Возможные объекты воздействия угроз безопасности информации

Негативные последствия, объекты воздействия, виды воздействия на них в ИСПДн «Кадры» ЗАО «Солнышко» изображены в таблице 5[13].

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	Перехват информации, содержащей

[13] Пример определения объектов воздействия и видов воздействия на них приведен в Приложении 5 к Методике оценки угроз безопасности информации: методический документ, утвержден ФСТЭК России 5 февраля 2021 г. – М.: 2021. – 83 с. – Текст : электронный // Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и подготовленные проекты документов по технической защите информации online. – URL: https://fstec.ru/component/attachments/download/2919.

	сервером основного центра обработки данных и сервером резервного центра обработки данных Веб-приложение информационной системы, обрабатывающей идентификационную информацию граждан	идентификационную информацию граждан, передаваемой по линиям связи Несанкционированный доступ к идентификационной информации граждан, содержащейся в веб-приложении информационной системы

5. Источники угроз безопасности информации

Возможные цели реализации угроз безопасности ПД в ИСПДн «Кадры» ЗАО «Солнышко» нарушителями[14] 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

[14] Пример определения возможных целей реализации угроз безопасности информации нарушителями приведен в Приложении 6 к Методике оценки угроз безопасности информации: методический документ, утвержден ФСТЭК России 5 февраля 2021 г. – М.: 2021. – 83 с. – Текст : электронный // Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и подготовленные проекты документов по технической защите информации online. – URL: https://fstec.ru/component/attachments/download/2919.

Уровни возможностей нарушителей по реализации угроз безопасности ПД в ИСПДн «Кадры» ЗАО «Солнышко» представлена в таблице 7[15].

Таблица 7

№	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. Имеет возможность использовать средства реализации угроз (инструменты), свободно распространяемые в сети "Интернет" и разработанные другими лицами, имеет минимальные знания механизмов их функционирования, доставки и выполнения вредоносного программного обеспечения, эксплойтов. Обладает базовыми компьютерными знаниями и навыками на уровне пользователя.	Физическое лицо (хакер) Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем. Лица, обеспечивающие функционирование систем и сетей или обеспечивающих систем (администрация, охрана, уборщики и т.д.) Авторизованные пользователи систем и сетей Бывшие работнии (пользователи)

[15] Пример оценки целей реализации нарушителями угроз безопасности информации в зависимости от возможных негативных последствий и видов ущерба от их реализации (для ГИС) приведен в Приложении 7 к Методике оценки угроз безопасности информации: методический документ, утвержден ФСТЭК России 5 февраля 2021 г. – М.: 2021. – 83 с. – Текст : электронный // Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и подготовленные проекты документов по технической защите информации online. – URL: https://fstec.ru/component/attachments/download/2919.

		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	

6. 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[16].

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

Таблица 8

№	Вид	Категория	Объект	Доступные	Способы

[16] Примеры определения актуальных способов реализации угроз безопасности информации и соответствующие им виды нарушителей и их возможности приведен в Приложении 7 к Методике оценки угроз безопасности информации: методический документ, утвержден ФСТЭК России 5 февраля 2021 г. – М.: 2021. – 83 с. – Текст : электронный // Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и подготовленные проекты документов по технической защите информации online. – URL: https://fstec.ru/component/attachments/download/2919.

п/п	нарушителя	нарушителя	воздействия	интерфейсы	реализации
1	Разработчики программных, программно-аппаратных средств	Внешний	ПО	Удаленное подключение	внедрение дополнительных функциональных возможностей в программные или программно-аппаратные средства

7. Актуальные угрозы безопасности информации

7.1 Актуальные техники и тактики реализации угроз.

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[17].

Таблица 9 – Расшифровка актуальных техник и тактик реализации УБИ

№	Тактика	Основные техники
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

[17] Пример Переченя основных тактик и соответствующих им типовых техник, используемых для построения сценариев реализации угроз безопасности приведен в Приложении 11 к Методике оценки угроз безопасности информации: методический документ, утвержден ФСТЭК России 5 февраля 2021 г. – М.: 2021. – 83 с. – Текст : электронный // Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и подготовленные проекты документов по технической защите информации online. – URL: https://fstec.ru/component/attachments/download/2919.

7.2 Перечень актуальных угроз безопасности информации

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 несанкционированной модификации защищаемой информации	Н2	Прикладное программное обеспечение, Платежная\ финансовая информация	С1,С10,С12	П2.2
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

Таким образом, в отношении персональных данных, обрабатываемых в ИСПДн «Кадры» ЗАО «Солнышко»», актуальными являются следующие угрозы безопасности[18]:

1. Угрозы несанкционированной модификации защищаемой информации
2. Угрозы внесения несанкционированных изменений в прикладное ПО
3. Угрозы сбора информации защищаемой системы
4. Угрозы ошибочных действий

Экспертная группа:

Начальник отдела ИБ ЗАО «Солнышко»	Семенов С.С.
Начальник отдела аудита ФГУП «НПП «Бэтта»	Васильев Р.А.
Ведущий специалист по ТЗИ ФГУП «НПП «Бэтта»	Петров В.И.

[18] Перечислить актуальные угрозы безопасности