**МИНОБРНАУКИ РОССИИ**

**САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ**

**ЭЛЕКТРОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ**

**«ЛЭТИ» ИМ. В.И. УЛЬЯНОВА (ЛЕНИНА)**

**Кафедра ИБ**

**ОТЧЕТ**

**по практической работе №1**

**по дисциплине «Технология разработки ИС в ЗИ»**

**ТЕМА: Предпроектное обследование ИС**

|  |  |  |
| --- | --- | --- |
| Студенты гр. 3361 |  | Воловик П. А. |
|  |  | Столетов А. С. |
|  |  | Субботин Д.А |
| Преподаватель |  | Березин А.Н. |

Санкт-Петербург

2018

**Цель работы.**

Получить практические навыки проведения предпроектного обследования ИС и составления документов по его результатам.

**Теоретические сведения.**

Цель системы защиты – устранение угроз или ослабление их действия на защищаемую систему до приемлемого уровня.

1. Предотвращение материального ущерба, незапланированных трудозатрат.

2. Обеспечение устойчивого (бесперебойного) функционирования ОИ.

3. Исключение или снижение возможности возникновения, реализации угроз ИБ.

Работы по созданию/модернизации системы защиты информации ИС – являются неотъемлемой частью работ по созданию ИС, ее эксплуатации или модернизации.

Концепция ИБ предприятия должна опираться на действующие нормативно-правовые акты, руководящие документы регуляторов, в том числе на концепцию и политику ИБ ведомства (отрасли).

Документирование включает в себя:

1. Отчет о результатах обследования.
2. Техническое задание (на систему в целом).
3. Частные техзадания (на части системы).
4. Технический проект. Технорабочий проект.
5. Рабочая документация.
6. Эксплуатационная (объектовая) документация.

В ходе данной лабораторной рассматривается пункт №1 – отчет о результатах обследования.

Порядок выполнения работ при построении системы защиты информации для действующей информационной системы:

1. подготовительный этап выполнения работ;
2. стадия обследования (обследование ИСПДн, процессов обработки ПДн, классификация ИСПДн, разработка модели угроз и нарушителя);
3. этап разработки (дополнения) организационно-распорядительных документов;
4. стадия проектирования СЗПДн, включая разработку технического проекта;
5. этап ввода в эксплуатацию СЗПДн;
6. оценка эффективности реализованных мер защиты ПДн (приемочные испытания, период. контроль).

В этой работе подробно рассмотрен подготовительный этап выполнения работ.

Подготовка к обследованию ИС включает в себя:

1. Определение сроков и стоимости проекта.

2. Назначение рабочей группы.

3. Выбор исполнителя – собственными силами или аутсорсинговой организации.

Методы обследования системы:

1. Документационный – трудоемкий, достоверность низкая (документы зачастую не обновляются).
2. Анкетирование – наиболее применим в крупных компаниях, в случае хорошей организации занимает мало времени.
3. Интервьюирование – наиболее достоверный метод обследования. В случае небольших компаний целесообразно сразу проводить интервьюирование. В крупных компаниях проводится выборочное интервьюирование по результатам анкетирования.

В нашей работе будет использоваться первый метод – документационный.

Обследование системы:

1. анализ внутренних нормативных документов о порядке обработки и защиты ПДн;
2. определение перечня ПДн, подлежащих защите;
3. определение перечня ИС, обрабатывающих ПДн;
4. определение класса ИСПДн;
5. определение используемых средств защиты ПДн, и оценка их соответствия требованиям нормативных документов РФ;
6. разработка модели нарушителя;
7. разработка частной модели угроз информационной безопасности ПДн.

Обследование системы методом анкетирования:

1. Субъекты ПДн (работники, клиенты, контрагенты и т.д.).
2. Состав ПДн для каждого субъекта (ФИО, паспорт и т.д.).
3. Основания и цели обработки.
4. Вид обработки (в ИСПДн, без использования средств автоматизации).
5. Места хранения ПДн (в электронном/бумажном виде).
6. Откуда поступают и куда передаются ПДн.
7. Процессы, связанные с обработкой (сбор согласий, анкетирование и т.д.).
8. Физическая защита ПДн.
9. Регламентация доступа к ПДн.
10. Информационные системы и операции с ПДн в них.

Описание ИС при обследовании:

1. Перечень утвержденных политик, положений, регламентов, процедур, инструкций в части обеспечения безопасности информации.
2. Описание внешних каналов связи (провайдеры услуг, взаимодействие со сторонними организациями).
3. Описание резервных каналов связи (при наличии).
4. Описание средств и порядка разграничения доступа пользователей к сети Интернет (возможно, описание содержится в соответствующем нормативном документе).
5. Порядок разграничения доступа к параметрам BIOS, параметрам ОС и ППО. Описание VLAN (при наличии).
6. Распределение ролей между подразделениями и сотрудниками в ИТ-инфраструктуре (например, ответственным за тех. поддержку пользователей ИС является \_\_\_\_\_, за выполнение резервного копирования – \_\_\_\_\_, за обеспечение безопасности информации –\_\_\_\_ и т.д.).
7. Физическая защита (организационные меры и технические средства разграничения физического доступа, расположение помещений с коммуникационным и серверным оборудованием; описание физической защищенности данных помещений; перечень лиц, имеющих доступ).
8. Доменная структура.
9. Активное сетевое оборудование (физическая и логическая структура). Серверное оборудование.
10. Рабочие станции пользователей.
11. Защита периметра (межсетевые экраны).
12. Виртуализация.

Кроме того, для правильного заполнения шаблонов документов необходимо учесть следующие особенности:

* 1. В перечне документов по ПДн в организации описываются документы, разработанные в вашей организации, по обработке и защите ПДн (напр., форма согласия субъекта ПДн на обработку ПДн). Если не разработаны, оставьте таблицу пустой. Если в вашей организации более 1 ИСПДн и документ относится к конкретной ИСПДн, то указывать в этом списке его не нужно.
  2. Если в организации не используются средства криптографической защиты, то заполнение таблиц А.8 с вопросами по ФАПСИ 152, А.16 с вопросами по ФСБ 378 и А.17 с вопросами по ФАПСИ 152 не требуется.
  3. В сведениях об ИСПДн заполняется всё касательно только 1 ИСПДн, если в организации 2 и более ИСПДн, то данные вопросы копируются и добавляются в конец документа, а затем заполняются для последующих ИСПДн.

Постановка задачи.

Выполнить все шаги работы, необходимые для осуществления предпроектного обследования ИС. Результаты зафиксировать в отчете.

ОРГАНИЗАЦИОННАЯ СТРУКТУРА

Организация ООО «НСТ» имеет следующие отделы:

1. Отдел кадров
2. Финансовый отдел
3. IT отдел
4. Рабочие группы

ОРГАНИЗАЦИОННАЯ СТРУКТУРА ПЕРСОНАЛА

1. Отдел кадров:
   1. Начальник отдела кадров
   2. Кадровый специалист
2. Финансовый отдел:
   1. Главный бухгалтер
   2. Специалист по банковским операциям
3. IT отдел:
   1. Системный администратор
   2. Специалист ИБ
4. Рабочие группы:
   1. Начальник группы
   2. Менеджер обработки данных (оператор)

Утверждаю:

Согласовано:

Директор

ООО «НСТ»

Бобриков М. В.

«15» февраля 2018 год

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

«15» февраля 2018 год

# ОБЩИЕ СВЕДЕНИЯ ОБ ОРГАНИЗАЦИИ, ОБРАБАТЫВАЮЩЕЙ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

СВЕДЕНИЯ ОБ ОРГАНИЗАЦИИ

Таблица А.1 – Сведения об организации

|  |  |  |
| --- | --- | --- |
| **№№** | **Описание** | **Значение** |
| 1 | Название организации | Контактный центр «SoCall» |
| 2 | Адрес организации | |  | | --- | | Санкт-Петербург, ул. Льва Толстого, д.9, девятый этаж, помещение 912 | |
| 3 | Сокращенное название организации | ООО «НСТ» |
| 4 | Телефон организации, контактное лицо | 8 905 231 95 35, Бобриков М. В. |
| 5 | Сфера деятельности | Техническая поддержка автоматизированных систем |
| 6 | Характер выполняемой работы | Краудсорсинг |
| 7 | По географическому признаку | Объектовая |
| 8 | По организационному признаку | Механистическое |

СВЕДЕНИЯ О ЗАНИМАЕМЫХ ПОМЕЩЕНИЯХ

Таблица А.2 – Сведения о занимаемых помещениях

|  |  |  |
| --- | --- | --- |
| **№№** | **Описание** | **Значение** |
| 1 | Форма собственности (аренда, собственное здание и т.д.) | Аренда помещения |
| 2 | Присутствуют ли сторонние организации в том же здании и/или на том же этаже? | Отсутствуют |

СВЕДЕНИЯ ОБ ОХРАНЕ ПОМЕЩЕНИЙ ОРГАНИЗАЦИИ

Таблица А.3 – Сведения об охране помещений организации

|  |  |  |
| --- | --- | --- |
| **№№** | **Описание** | **Значение** |
| 1 | Кто осуществляет охрану помещений (ведомственная, вневедомственная охрана, собственник здания и т.д.)? | Собственник здания |
| 2 | Есть ли технические средства – датчики движения, проникновения (внутри и по периметру здания)? | Есть внутри здания |
| 3 | Ведется ли видеонаблюдение (внутри и по периметру здания)? | Ведётся внутри помещений |
| 4 | Используются ли персональные средства идентификации на входе в здание (пропуска, смарткарты и т.д.)? | Используются пропуски |

от Заказчика \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ от Исполнителя \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Используемые сокращения

**ПДн** – персональные данные. **В соответствии с п.1 статьи 3ФЗ №152. Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).**

**ИСПДн** – информационная система персональных данных.

**СЗИ** – средство защиты информации.

**СКЗИ** – средство криптографической защиты информации.

**АРМ** – автоматизированное рабочее место.

**СОВ** – система обнаружения вторжений.

**МЭ** – межсетевой экран.

**СЗИ НСД** – средство защиты от несанкционированного доступа.

**СТР-К** – специальные требования и рекомендации по технической защите конфиденциальной информации

**КЗ** – контролируемая зона

перечень Документов по ПДн в организации

Таблица А.4

|  |  |
| --- | --- |
| **№№** | **Название документа** |
|  | Форма уведомления об обработке ПД (согласно ФЗ№152 от 27.07.06, ст.22) |
|  | Форма согласия субъекта ПД на обработку его ПД (согласно ФЗ№152 от 27.07.06, ст.9) |
|  | Форма разъяснения субъекту ПД юридических последствий отказа предоставить свои ПД |
|  | Форма обязательства работника, непосредственно осуществляющего обработку ПД, о прекращении обработки ПД, ставших известных ему в ходе исполнения им своих должностных обязанностей, в случае расторжения с ним договора. |
|  | Форма акта приема-передачи документов, содержащих ПД субъектов |
|  | Форма акта «об уничтожении ПД субъектов при достижении целей обработки» |
|  | Проект уведомления о начале обработки ПД для предоставления в территориальный орган Роскомнадзора |
|  | Правила организации обработки и осуществления защиты ПД, обрабатываемых без использования средств автоматизации |
|  | Приказ «об утверждении формы согласия на обработку персональных данных, уведомления об обработке персональных данных физического лица, уведомления об устранении нарушений, допущенных при обработке персональных данных и уведомления об уничтожении персональных данных физического лица» |
|  | Приказ «о назначении ответственного за организацию обработки персональных данных у оператора» (согласно ФЗ№152 от 27.07.06, ст.22) |
|  | Должностная инструкция ответственного лица за организацию обработки ПД |
|  | Приказ «об утверждении перечней обрабатываемых ПД» |
|  | Приказ «об утверждении перечня лиц, имеющих право доступа в помещения, в которых ведется обработка ПД» |
|  | Правила доступа работников в помещения, в которых ведется обработка ПД |
|  | Проект руководства администратора ИСПД |
|  | Проект руководства пользователя ИСПД |
|  | Приказ «об утверждении мест хранения материальных носителей ПД» |
|  | Типовой план мероприятий по защите ПД |
|  | Типовой план внутренних проверок состояния обработки и защиты ПД |
|  | Приказ «о назначении комиссии, осуществляющей внутренние проверки состояния обработки и защиты ПД» |
|  | Приказ «об использовании электронных журналов, а также об утверждении перечня используемых электронных журналов и лиц, допущенных к ним» |
|  | Журнал учета материальных носителей, предназначенных для хранения ПД |

от Заказчика \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ от Исполнителя \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Продолжение таблицы А.4

|  |  |
| --- | --- |
| **№№** | **Название документа** |
|  | Журнал учета обращений субъектов ПД и их законных представителей |
|  | Журнал учета выдачи материальных носителей, содержащих ПД |
|  | Приказ «об утверждении форм бланков, связанных с процессами обработки ПД (бланк уведомления субъекта о начале обработки его ПД, бланк запроса субъекта на получение доступа к своим ПД и т.п.)» |
|  | Приказ «об утверждении перечня лиц, допущенных к работе с СКЗИ» |
|  | Журнал инструктажа по работе с СКЗИ |
|  | Приказ «об утверждении перечня лиц, имеющих доступ к ПДн» |
|  | Приказ «об утверждении перечня лиц, осуществляющих обработку ПДн» |
|  | Электронный журнал действий пользователей ИСПДн |
|  | Электронный журнал полномочий сотрудников оператора ПДн по доступу к ПДн |
|  | Электронный журнал сообщений |
|  | Приказ «о назначении ответственного за контроль ведения электронного журнала полномочий сотрудников оператора персональных данных по доступу к персональным данным лица» |
|  | Журнал поэкземплярного учета СКЗИ, эксплуатационной и технической документации и ключевых документов |
|  | Технический журнал регистрации криптографических ключей |
|  |  |
|  |  |
|  |  |

Вопросы по ПП1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных"

Таблица А.5

|  |  |  |
| --- | --- | --- |
| **№№** | **Описание** | **Значение** |
|  | Назначено ли ответственное за организацию обработки ПДн должностное лицо? | Назначено |
|  | Организовано ли структурное подразделение ответственное за обеспечения безопасности ПДн? | Организовано |
|  | Осуществляется ли в организации обработка ПДн полученных из общедоступных источников? | Осуществляется |
|  | Осуществляется ли периодический контроль соответствия требования ПП1119? | Не осуществляется |

Вопросы по ПП687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации"

Таблица А.6

|  |  |  |
| --- | --- | --- |
| **№№** | **Описание** | **Значение** |
|  | Проводится ли в организации инструктаж сотрудников, осуществляющих обработку ПДн без использования средств автоматизации о правилах и особенностях такой обработки? | Проводится |
|  | Производится ли в организации сбор каких-либо персональных данных для однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, или в иных аналогичных целях? | Проводится |

от Заказчика \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ от Исполнителя \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Вопросы по ФЗ 152 "О персональных данных"

Таблица А.7

|  |  |  |
| --- | --- | --- |
| **№№** | **Описание** | **Значение** |
|  | Запрашивается ли у субъекта ПДн в каком-либо виде согласие на их обработку? | Запрашивается |
|  | Обеспечен ли неограниченный доступ к документу определяющему политику организации в отношении обработки персональных данных? | Обеспечен |
|  | Осуществляется ли внутренний контроль(аудит) соответствия процесса обработки ПДн требованиям законодательства? | Не осуществляется |
|  | Осуществляется ли контроль за примененными мерами по обеспечению безопасности? | Осуществляется |
|  | Осуществляется ли уведомление уполномоченного органа по защите прав субъекта в случае прекращения обработки? | Осуществляется |
|  | Отправляли ли уведомление о начале обработки ПДн в Роскомнадзор? | Отправляли |
|  | Предоставляются ли субъекту по его просьбе данные касающейся обработки его ПДн? | Предоставляются |
|  | Принимаются ли на основании исключительно автоматизированной обработки решения, имеющие юридические последствия? | Не принимаются |

Продолжение таблицы А.7

|  |  |  |
| --- | --- | --- |
|  | Проводится ли ознакомление сотрудников оператора, осуществляющих обработку ПДн с положениями законодательства в сфере ПДн? | Проводится |
|  | Разъясняются ли субъекту ПДн юридические последствия в случае отказа от их предоставления (если предоставление ПДн является обязательный в соответствии в ФЗ)? | Разъясняются |

Вопросы по ФАПСИ 152 "Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну"

Таблица А.8

|  |  |  |
| --- | --- | --- |
| **№№** | **Описание** | **Значение** |
|  | Передаётся ли конфиденциальная информация, защищенная с использованием средств СКЗИ вне сетей конфиденциальной связи? | Не передаётся |
|  | Передаются ли по техническим средствам связи служебные сообщения, касающиеся организации и обеспечения безопасности хранения? | Не передаются |
|  | Проводится ли обучение должностных лиц, допущенных к работе с СКЗИ? | Проводится |
|  | Утвержден ли перечень лиц, допущенных к работе с СКЗИ? | Утверждён |

от Заказчика \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ от Исполнителя \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**СВЕДЕНИЯ ОБ ИНФОРМАЦИОННОЙ СИСТЕМЕ ПЕРСОНАЛЬНЫХ ДАННЫХ (ИСПДн«БД сотрудников ООО «НСТ»»**

Таблица А.9 – Общие сведения об ИСПДн

|  |  |  |
| --- | --- | --- |
| **№№** | **Описание** | **Значение** |
|  | Название ИСПДн | БД сотрудников ООО «НСТ» |
|  | Персональные данные граждан РФ хранятся на территории РФ? | ПДн хранятся на территории РФ |
|  | Занимаемые помещения (списком с адресами) | Санкт-Петербург, ул. Льва Толстого, д.9, девятый этаж, помещение 912 |
|  | Взаимодействие с другими ИСПДн? | Отсутствует |
|  | Предусмотрено ли акустическое воспроизведение ПДн (или голосовой ввод ПДн) в ИСПДн? | Не предусмотрено |
|  | Присутствует ли в ИСПДн подсистема печати? | Присутствует |
|  | Есть ли доступ в общедоступные сети (интернет) с компьютеров, на которых производится обработка персональных данных? | Отсутствует |
|  | Используются ли технологии беспроводного доступа при обработке ПДн (Wi-Fi)? | Не используются |
|  | Существует ли возможность подключить к техническим средствам ИСПДн мобильный телефон, КПК, цифровую камеру по какому-либо интерфейсу? | Отсутствует |
|  | Производится ли своевременное обновление ПО, установка патчей и "заплаток"? | Производится |

Таблица А.10 – Характеристики ИСПДн

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№№** | **Наименование** | **Описание** | **Значение** | **Выбрать** |
| 1 | Категория ПДн | Специальные | ПДн, касающиеся расовой, национальной принадлежности, политических, религиозных и философских убеждений, состояния здоровья, интимной жизни |  |
| Биометрические | ПДн, характеризующие биологические или физиологические особенности субъекта, например, фотография или отпечатки пальцев |  |
| Общедоступные | Сведения о субъекте, полный и неограниченный доступ к которым предоставлен самим субъектом | + |
| Иные | Не представленные в трех предыдущих группах | + |
| 2 | Объем ПДн | 1 | В информационной системе одновременно обрабатываются персональные данные более чем 100 000 субъектов персональных данных |  |
| 2 | В информационной системе одновременно обрабатываются персональные данные менее чем 100 000 субъектов персональных данных | + |
| 3 | Субъекты ПДн | 1 | Сотрудники организации (люди, связанные с организацией трудовыми отношениями) | + |
| 2 | Не сотрудники организации (люди, не связанные с организацией трудовыми отношениями) |  |

от Заказчика \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ от Исполнителя \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Сведения о СУБЪЕКТах ПДн и обрабатывющих ПДН СОТРУДНИКАХ

Таблица А.11

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **№№** | **Субъекты персональных данных** | **На основании чего ведётся обработка** | **Категории персональных данных (**Ф.И.О., паспортные данные, ИНН, данные об образовании, данные о состоянии здоровья и т.д.**)** | **Должность обрабатывающего ПДн сотрудника** | **Структурное подразделение, к которому относится сотрудник** | **Перечень производимых действий с ПДн** |
|  | Начальник отдела кадров | Федеральный закон РФ от 27.07.2006 № 152-ФЗ "О персональных данных", п.п. 3, 10, 17 таблицы А.4 | ФИО, паспортные данные, ИНН, данные регистрации, телефон, email, данные об образовании, должность, оклад, банковский зарплатный счет | Кадровый специалист, Специалист по банковским операциям | Кадровый отдел | Внесение, редактирование ПДн, просмотр, удаление, блокирование |
|  | Сотрудник отдела кадров | Федеральный закон РФ от 27.07.2006 № 152-ФЗ "О персональных данных" | ФИО, паспортные данные, ИНН, данные регистрации, телефон, email, данные об образовании, должность, оклад, банковский зарплатный счет | Кадровый специалист, Специалист по банковским операциям | Кадровый отдел | Внесение, редактирование ПДн, просмотр, удаление, блокирование |
|  | Главный бухгалтер | Федеральный закон РФ от 27.07.2006 № 152-ФЗ "О персональных данных" | ФИО, паспортные данные, ИНН, данные регистрации, телефон, email, данные об образовании, должность, оклад, банковский зарплатный счет | Кадровый специалист, Специалист по банковским операциям | Финансовый отдел | Внесение, редактирование ПДн, просмотр, удаление, блокирование |
|  | Системный администратор | Федеральный закон РФ от 27.07.2006 № 152-ФЗ "О персональных данных" | ФИО, паспортные данные, ИНН, данные регистрации, телефон, email, данные об образовании, должность, оклад, банковский зарплатный счет | Кадровый специалист, Специалист по банковским операциям | IT-отдел | Внесение, редактирование ПДн, просмотр, удаление, блокирование |
|  | Специалист ИБ | Федеральный закон РФ от 27.07.2006 № 152-ФЗ "О персональных данных" | ФИО, паспортные данные, ИНН, данные регистрации, телефон, email, данные об образовании, должность, оклад, банковский зарплатный счет | Кадровый специалист, Специалист по банковским операциям | IT-отдел | Внесение, редактирование ПДн, просмотр, удаление, блокирование |
|  | Начальник группы | Федеральный закон РФ от 27.07.2006 № 152-ФЗ "О персональных данных" | ФИО, паспортные данные, ИНН, данные регистрации, телефон, email, данные об образовании, должность, оклад, банковский зарплатный счет | Кадровый специалист, Специалист по банковским операциям | Отдел по работе с клиентами | Внесение, редактирование ПДн, просмотр, удаление, блокирование |
|  | Операторы | Федеральный закон РФ от 27.07.2006 № 152-ФЗ "О персональных данных", п.п. 3, 10, 18 таблицы А.4 | ФИО, паспортные данные, ИНН, данные регистрации, телефон, email, данные об образовании, должность, оклад, банковский зарплатный счет | Кадровый специалист, Специалист по банковским операциям | Отдел по работе с клиентами | Внесение, редактирование ПДн, просмотр, удаление, блокирование |

от Заказчика \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ от Исполнителя \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Вопросы по ПП1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных"**

Таблица А.12

|  |  |  |
| --- | --- | --- |
| **№** | **Описание** | **Значение** |
|  | Актуальны ли для вашей ИСПДн угрозы недекларированных возможностей в прикладном ПО на АРМ где ведется обработка и хранение ПДн? | Актуальны |
|  | Актуальны ли для вашей ИСПДн угрозы недекларированных возможностей в системном ПО на АРМ где ведется обработка и хранение ПДн? | Не актуальны |
|  | Организован ли доступ к содержанию электронного журнала сообщений исключительно для должностных лиц (работников) оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей? | Организован |
|  | Осуществляется ли выбор средств защиты в соответствии с законодательством РФ в сфере зашиты ПДн? | Не осуществляется |
|  | Производится ли автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным? | Производится |
|  | Производится ли определение типа угроз безопасности ПДн соответствии с законодательством в сфере защиты ПДн? | Не производится |
|  | Утвержден ли перечень лиц, доступ которых к ПДн необходим для выполнения ими служебных обязанностей? | Утвержден |

**Вопросы по ПП687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации"**

Таблица А.13

|  |  |  |
| --- | --- | --- |
| **№** | **Описание** | **Значение** |
|  | Осуществляется ли в ИСПДн обработка ПДн без использования средств автоматизации? | Осуществляется |
|  | Используются ли типовые формы для заполнения, которые предполагают или допускают включение в них ПДн? | Используются |
|  | Обеспечена ли фиксация персональных данных, обрабатываемых в разных целях, на разных материальных носителях? | Обеспечена |
|  | Обеспечено ли обособление ПДн от иной информации? | Обеспечено |
|  | Обеспечено ли раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях? | Обеспечена |
|  | Определен ли перечень лиц, имеющих доступ к ПДн? | Определен |
|  | Определен ли перечень лиц, осуществляющих обработку ПДн? | Определен |
|  | Определены ли места хранения ПДн (материальных носителей)? | Определены |
|  | Присутствуют ли в ИСПДн материальные носители, на которых указаны ПДн, обрабатываемые с разными целями? | Отсутствуют |
|  | Можно ли определить в отношении каждой категории персональных данных места их хранения? | Можно |

от Заказчика \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ от Исполнителя \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Вопросы по ФСТЭК21 "ОБ УТВЕРЖДЕНИИ СОСТАВА И СОДЕРЖАНИЯ ОРГАНИЗАЦИОННЫХ И ТЕХНИЧЕСКИХ МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ"**

Таблица А.14

|  |  |  |
| --- | --- | --- |
| **№** | **Описание** | **Значение** |
|  | Ведётся ли журнал учёта машинных носителей ПДн? | Да |
|  | Ведется ли электронный журнал действий пользователей ИСПДн? | Да |
|  | Есть ли возможность заглянуть в помещение, где есть визуальное отображение информации (хотя бы через окно, дверь) постороннему человеку? | Нет |
|  | Имеется ли в ИСПДн журнал внутренних проверок состояния обработки и защиты ПДн? | Да |
|  | Имеется ли журнал внесения изменений конфигурации информационной системы и системы защиты ПДн? | Нет |
|  | Используется ли виртуальная инфраструктура для обработки ПДн? | Нет |
|  | Используются ли в ИСПДн сертифицированное ФСТЭК или ФСБ антивирусное программное обеспечение? | Да |
|  | Используются ли в ИСПДн сертифицированные ФСТЭК или ФСБ межсетевые экраны? | Да |
|  | Используются ли в ИСПДн сертифицированные ФСТЭК или ФСБ системы обнаружения вторжений? | Да |
|  | На всех компьютерах, обрабатывающих ПДн установлена система защиты информации от несанкционированного доступа? | Да |
|  | Применяется ли резервное копирование защищаемой и сопутствующей информации? | Да |
|  | Разработаны ли инструкции по выявлению инцидентов при обработке ПДн и реагированию на них? | Не разработаны |
|  | Существует ли пропускной режим в помещения, в которых находится ИСПДн? | Существует |

**Вопросы по ФЗ 152 "О персональных данных"**

Таблица А.15

|  |  |  |
| --- | --- | --- |
| **№** | **Описание** | **Значение** |
|  | Исполняются ли требования к защите ПДн обеспечивающие необходимый уровень защищенности? | Не известно |
|  | Назначено ли ответственное за организацию обработки ПДн должностное лицо? | Назначено |
|  | Обеспечена ли регистрация и учет всех действий, совершаемых с ПДн в ИС? | Обеспечена |
|  | Обрабатываются ли в ИСПДн ПДн, избыточные по отношению к целям обработки? | Не обрабатываются |
|  | Обрабатываются ли в ИСПДн ПДн, полученные не от субъекта ПДн? | Не обрабатываются |
|  | Определен ли для ИСПДн необходимый уровень защищенности? | Не определен |
|  | Определяются ли угрозы безопасности ПДн при их обработке в ИС? | Не определяются |
|  | Осуществляется ли контроль уровня защищенности ИСПДн? | Не осуществляется |
|  | Осуществляется ли прекращение обработки ПДн в случае достижения цели обработки? | Осуществляется |
|  | Осуществляется ли уничтожение ПДн в случае выявления неправомерной обработки? | Осуществляется |
|  | Осуществляется ли уничтожение ПДн в случае достижения целей обработки? | Осуществляется |

от Заказчика \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ от Исполнителя \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Продолжение таблицы А.15

|  |  |  |
| --- | --- | --- |
| **№** | **Описание** | **Значение** |
|  | Применяются ли в ИСПДн средства защиты информации, прошедшие в установленном порядке процедуру оценки соответствия? | Применяются |
|  | Применяются ли меры для предотвращения и обнаружения фактов НСД к ПДн? | Применяются |
|  | Применяются ли требуемые законодательством организационные и технические меры по обеспечению безопасности ПДн? | Не известно |
|  | Проводится ли восстановление ПДн в случае их несанкционированной модификации или уничтожения? | Проводится |
|  | Проводится ли обучение сотрудников оператора, осуществляющих обработку ПДн? | Проводится |
|  | Проводится ли оценка вреда, который может быть причинен субъектам ПДн? | Не проводится |
|  | Проводится ли оценка эффективности применяемых мер по обеспечению безопасности до их ввода в эксплуатацию? | Не проводится |
|  | Производится ли обезличивание ПДн в случае достижения цели обработки или в случае утраты в необходимости обработки? | Не проводится (проводится уничтожение (таблица выше)) |
|  | Установлены ли в организации правила доступа к ПДн? | Не установлены |
|  | Осуществляется ли трансграничная передача ПДн? | Не осуществляется |

от Заказчика \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ от Исполнителя \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Вопросы по ФСБ 378 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности"

Таблица А.16

|  |  |  |
| --- | --- | --- |
| **№№** | **Описание** | **Значение** |
|  | Есть ли в ИСПДн сейф для хранения съемных носителей ПДн? | Есть |
|  | Назначено ли в организации ответственное за контроль ведения электронного журнала полномочий сотрудников оператора персональных данных по доступу к персональным данным лицо? | Назначено |
|  | Оборудованы ли окна и двери в помещения, где размещены серверы ИС, а также окна на первых и последних этажах здания и окна, находящиеся около пожарных лестниц металлическими решетками, охранной сигнализацией или другими средствами, препятствующими неконтролируемому проникновению посторонних лиц в помещения? | Оборудованы |
|  | Организован ли режим доступа в помещения, в которых размещена конфиденциальная информация, предотвращающий пребывание лиц, не имеющих права доступа в эти помещения? | Организован |
|  | Оснащена ли ИСПДн автоматическими средствами, исключающими доступ к содержанию электронного журнала сообщений лиц, регистрирующих запросы пользователей информационной системы на получение персональных данных, а также факты предоставления персональных данных по этим запросам, не указанных в утвержденном руководителем оператора списке лиц, допущенных к содержанию электронного журнала сообщений? | Оснащена |
|  | Оснащены ли помещения, где ведется обработка ПДн входными дверьми с замками и обеспечивается ли их (дверей) опечатывание в конце рабочего дня или иной контроль, за несанкционированным вскрытием помещения? | Оснащены |
|  | Осуществляется ли шифрование ПДн, находящихся на съемных носителях? | Осуществляется |
|  | Применяются ли в ИСПДн средства для автоматической регистрации запросов пользователей ИС на получение ПДн, а также фактов предоставления этих данных? | Применяются |
|  | Производится ли автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к ПДн? | Производится |
|  | Собираются ли данные для формирования совокупности предположений о направлениях возможных атак? | Собираются |
|  | Утвержден ли перечень лиц, имеющих право доступа в помещения, где ведется обработка ПДн? | Утверждён |
|  | Утвержден ли руководителем организации список должностных лиц, допущенных к работе с электронным журналом сообщений? | Утверждён |
|  | Утверждены ли правила доступа в помещения, где ведется обработка ПДн в нештатных ситуациях? | Утверждены |
|  | Утверждены ли правила доступа в помещения, где ведется обработка ПДн в рабочее и нерабочие время? | Утверждены |

от Заказчика \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ от Исполнителя \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Вопросы по ФАПСИ 152 "Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну"

Таблица А.17

|  |  |  |
| --- | --- | --- |
| **№№** | **Описание** | **Значение** |
|  | Ведется ли в ИСПДн журнал поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов? | Ведётся |
|  | Ведется ли в ИСПДн технический (аппаратный) журнал регистрации криптографических ключей? | Ведётся |
|  | Защищены ли окна помещений, где расположены СКЗИ от просмотра извне? | Защищены |
|  | Оснащены ли помещения, где расположены СКЗИ сигнализацией? | Оснащены |
|  | Осуществляется ли нумерация и учет ключей от помещений, где расположены СКЗИ, в журнале учета хранилищ? | Не осуществляется |
|  | Осуществляется ли отключение СКЗИ на время отсутствия пользователей данных средств или иная мера, исключающая возможность использования этих средств третьими лицами? | Осуществляется |
|  | Осуществляется ли периодическая проверка работоспособности сигнализации в помещениях, где расположены СКЗИ? | Осуществляется |

от Заказчика \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ от Исполнителя \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

перечень документов по обработке и защите ПДн, относящиеся к данной ИСПДн, разработанных в вашей организации (напр., матрица доступа)? (если не разработаны, оставьте таблицу пустой)

Таблица А.18

|  |  |
| --- | --- |
| **№№** | **Название документа** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

ПЕРЕЧЕНЬ ТЕХНИЧЕСКИХ СРЕДСТВ (ТС) И СВЕДЕНИЯ ОБ ИСПЛЬЗУЕМЫХ ОПЕРАЦИОННЫХ СИСТЕМАХ (ОС)

Таблица А.19

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Сведения об используемых технических средствах (автоматизированные рабочие места (АРМ), серверы, сетевое оборудование)** | | | | | |
| **№№** | **Наименование ТС** | **Класс ТС** | | | **Функции** | |
| 1 | Сервер | 7 | | | Обработка, передача, хранение информации  Отображение информации  Обработка, ввод информации  Вывод информации | |
| 2 |
| 3 |
| 4 |
| 5 | АРМ 1 | 7 | | | Обработка, передача, хранение информации  Отображение информации  Обработка, ввод информации  Вывод информации | |
| 6 |
| 7 |
| 8 |
| 9 | АРМ 2 | 7 | | | Обработка, передача, хранение информации  Отображение информации  Обработка, ввод информации  Вывод информации | |
| 10 |
| 11 |
| 12 |
| 13 | АРМ 3 | 7 | | | Обработка, передача, хранение информации  Отображение информации  Обработка, ввод информации  Вывод информации | |
| 14 |
| 15 |
| 16 |
| 17 | Сетевой принтер HP LaserJet P2015 | - | | | Вывод информации | |
| 5 | Маршрутизатор TP-LINK TL-WR841N | - | | | Передача информации | |
| **№№** | **Общее количество стационарных компьютеров / мобильных компьютеров / серверов** | | **Общее количество стационарных компьютеров / мобильных компьютеров / серверов, обрабатывающих ПДн** | | | |
| 1 | 4 | | 4 | | | |
|  | **Сведения об используемых операционных системах** **(АРМ, сервера)** | | | | | |
| **№№** | **Наименование ОС** | **Номер сертификата \*** | | **Срок действия сертификата \*** | | **Установлено на ТС №  (номера через запятую из таблицы выше)** |
| 1 | Операционная система Microsoft Windows 7 (SP1) в редакциях «Профессиональная», «Корпоративная» и «Максимальная» | 2180/1 | | 04.10.2018 | | 5,9,13 |
| 2 | Microsoft Windows server 2012 Database | 602 | | 15.06.2020 | | 1 |

Продолжение таблицы А.19

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Сведения об используемых программных средствах (АРМ, сервера)** | | | | | | **Категории персональных данных** |
| **№№** | **Наименование ПО** | **Номер сертификата** | **Срок действия сертификата** | **Функции** | **Размещение**  **(кабинет, этаж, здание)** | **Установлено на ТС №** |  |
| 2 | Oracle 8i Database Server | 602 | 15.06.2020 |  | 9 этаж, пом. 2113 | 1 | Иные (ФИО, паспортные данные, ИНН, данные регистрации, телефон, email, данные об образовании, должность, оклад, банковский зарплатный счет) |
| 3 | СУБД Oracle Database Personal Edition | - | - |  | 9 этаж, пом. 2113 | 5, 9, 13 | Иные (ФИО, паспортные данные, ИНН, данные регистрации, телефон, email, данные об образовании, должность, оклад, банковский зарплатный счет) |
| 4 | Microsoft Office 2016 Professional Plus | 3699 | 16.02.2020 |  | 2113 | 5, 9, 13 | Иные (ФИО, паспортные данные, ИНН, данные регистрации, телефон, email, данные об образовании, должность, оклад, банковский зарплатный счет) |
| 5 | Терьер 3.0 | 1193 | 05.07.2018 | Средство гарантированного уничтожения информации | 2113 | 1, 5, 9, 13 | Иные (ФИО, паспортные данные, ИНН, данные регистрации, телефон, email, данные об образовании, должность, оклад, банковский зарплатный счет) |

\* При отсутствии сертификата ФСТЭК или ФСБ поставить прочерк.

от Заказчика \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ от Исполнителя \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ПЕРЕЧЕНЬ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ (СЗИ)

Таблица А.20

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Сведения об используемых СЗИ** | | | | | |
| **Сведения об используемом антивирусном ПО** | | | | | |
| **№№** | **Наименование ПО** | **Номер сертификата \*** | **Срок действия сертификата \*** | **Класс сертификата** | **Установлено на ТС №** |
| 1 | Dr.Web Enterprise Security Suite версия 6.0 | 2446 | 20.09.2018 | НДВ 2 + ТУ | 5,9,13 |
| 2 | Антивирус Касперского 8.0 для Windows Servers Enterprise Edition | 2484 | 23.11.2018 | РД НДВ 2 + ТУ | 1 |
| **Сведения об используемых системах обнаружения вторжений (СОВ)** | | | | | |
| **№№** | **Наименование СОВ** | **Номер сертификата \*** | **Срок действия сертификата \*** | **Класс сертификата** | **Установлено на ТС №** |
| 1 | Рубикон | 2574 | 17.02.2018 | СОВ | 1,5,9,13 |
| **Сведения об используемых межсетевых экранах (МЭ)** | | | | | |
| **№№** | **Наименование МЭ** | **Номер сертификата \*** | **Срок действия сертификата \*** | **Класс сертификата** | **Установлено на ТС №** |
| 1 | Cisco ASA 5500 | 1719 | 17.11.2020 | РД МЭ(4) | 1,5,9,13 |
| **Сведения об используемых СЗИ от несанкционированного доступа к данным (СЗИ НСД)** | | | | | |
| **№№** | **Наименование СЗИ НСД** | **Номер сертификата \*** | **Срок действия сертификата \*** | **Класс сертификата** | **Установлено на ТС №** |
| 1 | Ревизор-2 ХР | 990 | 08.02.2020 | РД НДВ 2 + ТУ | 1,5,9,13 |
| **Сведения об используемых средствах криптографической защиты (СКЗИ)** | | | | | |
| **№№** | **Наименование СКЗИ** | **Номер сертификата \*** | **Срок действия сертификата \*** | **Класс сертификата** | **Установлено на ТС №** |
| 1 | Secret Net 7 | 2707 | 10.09.2018 | 2НДВ + 3 СВТ | 1,5,9,13 |

\* При отсутствии сертификата ФСТЭК или ФСБ поставить прочерк.

от Заказчика \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ от Исполнителя \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

описание процессов обработки ПДн

Таблица А.21

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Жизненный цикл ПДн в организации** | | Схема алгоритма обработки № 1 | | | Рис. 1 |
| **№№** | **Название операции** | **Задействованные лица** | **Используемые ТС** | **Используемое ПО** | **Описание процедуры** | |
| 1 | Сбор персональных данных | Субъекты ПДН | АРМ 1,2,3 | Misrosoft Office 2016 Professional Plus | Субъекты персональных данных предоставляют ПДН для последующей обработки. Предоставление данных осуществляется путем личной передачи, заполнения установленных законом и организацией форм. | |
| 2 | Обработка и ввод данных в БД | Менеджеры обработки ПДН  Кадровый специалист  Специалист по банковским опреациям | АРМ 1,2,3 Сервер | Misrosoft Office 2016 Professional Plus, СУБД Oracle Database Personal Edition | Осуществляется проверка, распределение и ввод ПДН в БД путем автоматизированным или без участия средств автоматизации. | |
| 3 | Машинная обработка | Менеджеры обработки ПДН | Сервер | СУБД Oracle Database Personal Edition | Загрузка ПДН в БД (сортировка, архивирование, поиск и т.п.) | |
| 4 | Хранение в БД и поддержка | Специалист ИБ, Системный администратор, | Сервер | СУБД Oracle Database Personal Edition | ПД хранятся в базе данных в течение срока установленного положением об обработке ПД в организации, но не противоречащему федеральным законам. В течение хранения ПД в базе данных осуществляется контроль за их защищенностью. | |
| 5 | Модификация ПДН | Менеджеры обработки ПДН  Кадровый специалист  Главный бухгалтер | АРМ 1,2,3 Сервер | Misrosoft Office 2016 Professional Plus, СУБД Oracle Database Personal Edition | Изменение ПДН по просьбе клиента в случаях их законного изменения (смена фамилия, мето работы и т.п.) | |
| 6 | Блокирование ПДН | Специалист ИБ, Системный администратор, | Сервер | СУБД Oracle Database Personal Edition | Блокирование доступа к ПДН и проведения всевозможных операций с ПДН в случае выявления их утечки, фальсификации или некорректности | |
| 7 | Уничтожение ПДН | Специалист ИБ Системный администратор, | Сервер | Терьер 3,0 | Уничтожение данных, если они стали не нужны, неактуальны или устарели. | |

от Заказчика \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ от Исполнителя \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**ОПИСАНИЕ ПРОЦЕССОВ ОБРАБОТКИ ПДН БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ**

Таблица А.22

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Процесс обработки ПДн без средств автоматизации** | | | **Схема алгоритма обработки № 1** | | **Рис. 2** |
| **№№** | **Название операции** | **Задействованные лица** | **Описание операции** | | **Обрабатываемые данные** | |
| 1 | Заполнение бланка формы с использованием ПДн (заявление на отпуск, заявление на увольнение и т.п.) | Субъект ПДн, кадровый специалист | Субъект ПДн заполняет необходимую форму, имеющую в своем содержании поля ПДн, в присутствии кадрового специалиста | | Общедоступные | |
| 2 | Фиксация материального носителя с ПДн обособленно от других носителей ПДн | Субъект ПДн, кадровый специалист | Субъект ПДн предоставляет ПДн, и подписывает согласие на обработку ПДн, которое хранится в бумажном виде в организации вместе с бланком формы | | Общедоступные | |
| 3 | Отказ в приеме ПДн у субъекта | Субъект ПДн, кадровый специалист | Если субъект ПДн отказывается подписать соглашение на обработку ПДн или вносит некорректные данные | | Общедоступные | |
| 4 | Принятие персональных данных у субъекта. | Субъект ПДн, кадровый специалист | Регистрация факта принятия ПДн с указанием даты в журнале. | | Общедоступные | |

от Заказчика \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ от Исполнителя \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

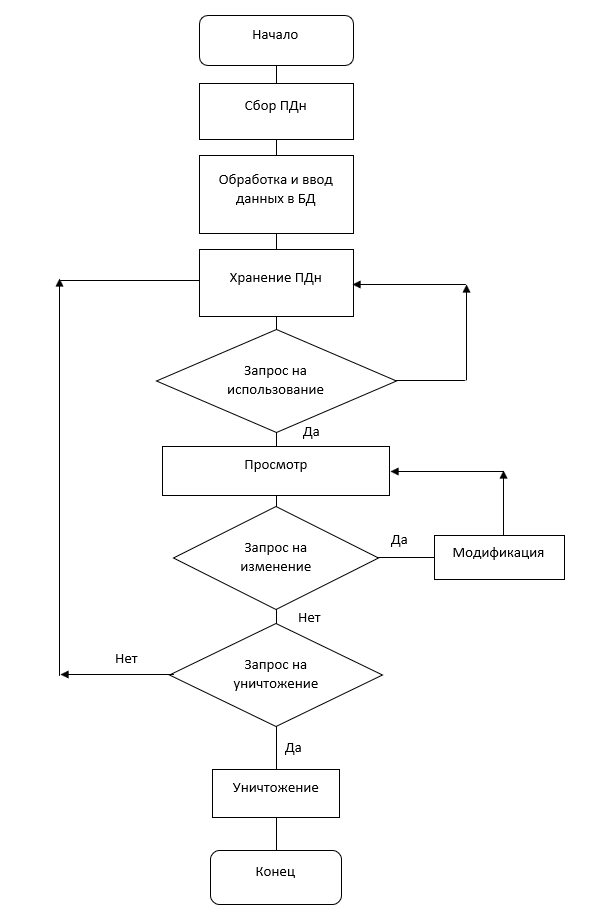


Рисунок 1 – Жизненный цикл ПДн в организации (с использованием средств автоматизации)

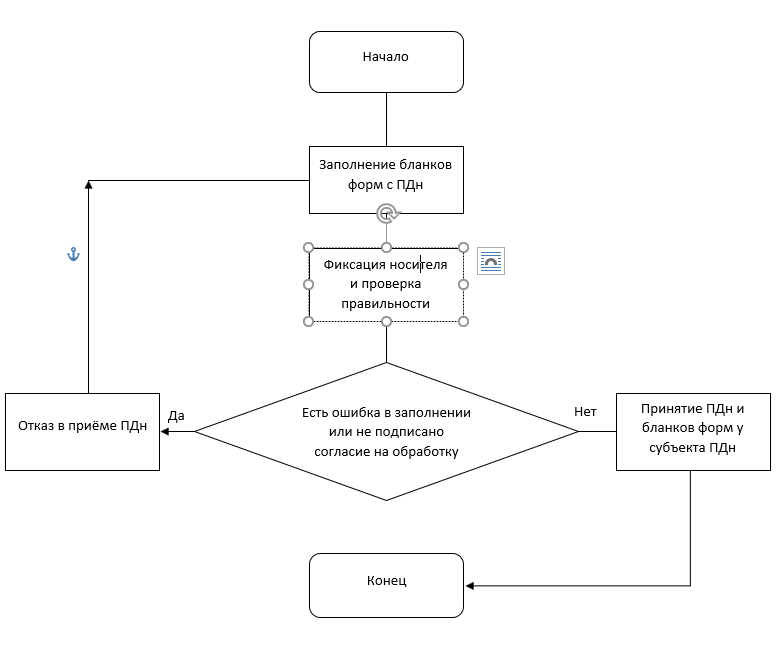


Рисунок 2 – Схема алгоритма обработки ПДн без использования средств автоматизации

**Вывод**

При выполнении данной лабораторной работы были получены практические навыки работы с документами, необходимыми для осуществления предпроектного обследования ИС, и непосредственно осуществлено данное обследование на примере организации ООО «НСТ», проведен анализ внутренних нормативных актов предприятия, перечень лиц, участвующих в процессах обработки ПДН, а также перечень и класс самих ПДН, фигурирующих в данной системе.

В ходе работы прошло ознакомление со многими нормативно-правовыми актами, регулирующими работу с ПДН в частности и с обеспечением информационной безопасности в целом. Данные документы отражены в списке литературы ниже.

По результатам работы обследование целевого объекта проведено, получена база для составления технического задания на создание защищенной ИСПДн.

В ходе обследования ИСПДн была выявлена необходимость разработки следующих документов:

* журнал внесения изменений конфигурации информационной системы и системы защиты ПДн;
* инструкции по выявлению инцидентов при обработке ПДн и реагированию на них;
* матрица доступа субъектов доступа к объектам доступа;
* акт классификации ИСПДн;
* технический паспорт информационной системы;
* методика оценки вреда, который может быть причинен субъектам ПДн;
* методика аудита процесса обработки ПДн по требованиям законодательства;

Также была выявлена необходимость проведения следующих мероприятий:

* нумерация и учет ключей от помещений, где расположены СКЗИ, в журнале учета хранилищ;
* выбор средств защиты в соответствии с законодательством РФ в сфере зашиты ПДн;
* контроль уровня защищенности ИСПДн;
* определение угроз безопасности ПДн при их обработке в ИС;

**Список литературы:**

1. Постановление Правительства Российской Федерации от 17.11.2007 г. №781 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»
2. Нормативно-методический документ ФСТЭК России «Рекомендации по обеспечению безопасности ПДн при их обработке в ИСПДн»
3. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)
4. Методический документ ФСТЭК «Рекомендации по обеспечению безопасности ПДн при их обработке в ИСПДн»
5. Федеральный закон «О персональных данных» ФЗ-152