Министерство образования и науки Российской Федерации

Федеральное государственное автономное образовательное

учреждение высшего образования

Национальный исследовательский университет “МИЭТ”

Институт Системной и программной инженерии и информационных технологий

1. Практическое занятие 3

**Дисциплина: Информационная безопасность**

Выполнили студенты П-32:

Селезнева Валерия  
Утева Александра

Москва, 2021

# Общие сведения

Настоящее Техническое задание (ТЗ) является основным документом, определяющим требования и порядок создания системы для защиты персональных данных автоматизированной системы АС «Pharmacy», в соответствии с которым проводится ее разработка и приемка при вводе в действие.

## **Полное наименование системы и ее условное обозначение**

Полное наименование системы Автоматизированная система «Pharmacy» ООО «Ромашка» (далее - АС «Pharmacy») категории АС 2Б (СВТ КЗ 5)

Условное обозначение системы: АС «Pharmacy».

## **Наименование предприятий разработчика и заказчика системы и их реквизиты**

Заказчик: ООО «Ромашка».

Адрес места нахождения: г. Клин, дом 8.

Фактический адрес: г. Клин, дом 8.

Исполнитель: АО «ЭЛВИС-ПЛЮС»

Адрес места нахождения: 620102, Российская Федерация, г. Екатеринбург, ул. Серафимы Дерябиной, д.20, 52. Фактический адрес: 620085, г. Екатеринбург, 8 марта, 205, каб. 316.

## **Перечень документов, на основании которых создается система**

Проводятся следующие этапы работ по созданию АС «Pharmacy»

|  |  |
| --- | --- |
| № п/п | Этапы работ по созданию АС |
| 1 | обследование процессов обработки персональных данных (ПДн) |
| 2 | построение Модели угроз безопасности ПДн |
| 3 | разработка ТЗ на создание АС |
| 4 | разработка Технического проекта |
| 5 | разработка ОРД по ПДн |
| 6 | разработка Рабочей документации |
| 7 | подготовка объекта автоматизации к вводу АС в действие |
| 8 | комплектация АС поставляемыми изделиями |
| 9 | строительно-монтажные работы |
| 10 | пуско-наладочные работы |
| 11 | аттестационные испытания АС |

.

Выполнение перечисленных выше этапов работ по организации обеспечения безопасности персональных данных ООО осуществляется в рамках следующих лицензий Исполнителя:

* лицензия ФСТЭК России на деятельность по технической защите конфиденциальной информации (бланк серия КИ 0066 № 003267, регистрационный № 1244 от 24.09.2018, действительна до 24.09.2023);
* лицензия ФСТЭК России на деятельность по разработке и (или) производству средств защиты конфиденциальной информации (бланк серия КИ 0066 № 003268, регистрационный № 0743 от 24.09.2018, действительна до 24.09.2023);
* лицензия УФСБ России по Свердловской области на осуществление

деятельности по распространению шифровальных (криптографических) средств (бланк серия ЛЗ № 0011980, регистрационный № 305Р от 10.08.2018, действительна до 10.08.2023);

* лицензия УФСБ России по Свердловской области на осуществление

деятельности по предоставлению услуг в области шифрования информации (бланк серия ЛЗ № 0011979, регистрационный № 307У от 10.08.2018,

действительна до 10.08.2023);

* лицензия УФСБ России по Свердловской области на осуществление деятельности по распространению шифровальных (криптографических) средств (бланк серия ЛЗ № 0011978, регистрационный № 306Х от 10.08.2018, действительна до 10.08.2023).

Остальные этапы работ по созданию СЗПДн АС " Pharmacy" проводятся в рамках отдельно заключаемых договоров.

## **Плановые сроки начала и окончания работ по созданию системы**

Сроки начала и окончания работ определяются условиями Коммерческого договора между Исполнителем и Заказчиком.

## **Порядок оформления и предъявления заказчику результатов работ по созданию системы**

Документация, предъявляемая Заказчику, должна быть разработана и оформлена в соответствии с требованиями следующих документов:

* + - Требования к защите персональных данных при их обработке в информационных системах персональных данных, утвержденные постановлением Правительства Российской Федерации от 1 ноября 2012 года

№ 1119;

* + - Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (утверждены приказом ФСТЭК России №21 от 18 февраля 2013 года);
    - ГОСТ Р 51583-2000 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения»;
    - ГОСТ 34.602-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы»;
    - ГОСТ 34.201-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем»;
    - ГОСТ 34.601-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания»;
    - РД 50-34.698-90 «Методические указания. Информационная технология. Комплекс Стандартов и руководящих документов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов».

# Назначение и цели создания системы

СЗПДн АС «Pharmacy» создается для исключения:

• неправомерного доступа, копирования, предоставления или распространения информационных ресурсов (обеспечение конфиденциальности информации);

• неправомерного уничтожения или модифицирования информационных ресурсов (обеспечение целостности информации);

• неправомерного блокирования информационных ресурсов (обеспечение доступности информации).

## **Цели создания системы**

Целью создания СЗПДн АС «Pharmacy» является снижение вероятности реализации угроз нарушения конфиденциальности, целостности и доступности в отношении ПДн, обрабатываемых в базе препаратов.

# Характеристика объекта автоматизации

В состав АСвходят следующие компоненты: СВТ, ИС, система хранения данных.

Подключенное к электрической системе питания СВТ обеспечивает функционирование локальной ИС, а также позволяет специалисту АС проводить все необходимые в ИС операции. Система хранения данных используется для хранения данных.

**Архитектура системы** не подразумевает масштабирования,т.е. развертывание новых виртуальных серверов. Для обеспечения бесперебойного функционирования системы используются источники бесперебойного питания. Администрирование системы осуществляется локально специалистом АС с правами.

**В ИС обрабатывается**: общедоступная (открытая) информация, доступная из сетей общего пользования (Интернет); информация конфиденциального характера (персональные данные), доступная из базы, данных защищенной АС.

**Защищаемая информация** размещена на базе АС установленной на ПК. Физически защищаемая информация расположена в системе хранения данных АС.

**В ИС подлежат защите** следующие ресурсы: программные и аппаратные средства (СВТ); система хранения данных с размещаемой на ней информацией конфиденциального характера, обрабатываемой информационной системой.

# Требования к системе

Автоматизированная система АС «Pharmacy» для обеспечения основных процессов ООО «Ромашка» должна предоставлять возможность сотрудникам:

* Видеть список препаратов в наличии/нет в наличии;
* Производить скидку на определённую категорию препаратов;
* Учета препаратов;

## **Требования к структуре и функционированию**

Структура АС «Pharmacy» должна включать подсистемы защиты информации, определяемые требованиям нормативных документов ФСТЭК России и ФСБ России в части безопасности ПДн и Моделью угроз безопасности ПДн.

Функции подсистем защиты информации СЗПДн АС «Pharmacy» должны быть направлены на защиту ПДн, обрабатываемых в АС, от угроз безопасности ПДн, приведенных в Модели угроз безопасности АС «Pharmacy» ПДн.

### **Перечень систем, подсистем, их назначение и основные характеристики**

Таблица 4.1 - Состав подсистем обеспечения безопасности

|  |  |  |  |
| --- | --- | --- | --- |
| №  п/п | Наименование подсистемы | Функции подсистемы | |
| 1 | Подсистема идентификации, проверки подлинности и контроля доступа субъектов | - идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов | |
| 2 | Подсистема регистрации и учета входа (выхода) субъектов доступа | - указывание даты и времени входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;  - результат попытки входа: успешная или неуспешная (при НСД); | |
| 3 | Подсистема учета носителей информации | - проведение учета всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку) | |
| 4 | Подсистема целостности программных средств и обрабатываемой информации | | - проверка целостности СЗИ НСД при загрузке системы по наличию имен (идентификаторов) компонент СЗИ  - обеспечение отсутствия в АС средств разработки и отладки программ во время обработки и (или) хранения защищаемой информации |
| 5 | Подсистема физической охраны средств вычислительной техники и носителей информации | | - осуществление физической охраны СВТ (устройств и носителей информации), предусматривающая контроль доступа в помещения АС посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения АС и хранилище носителей информации, особенно в нерабочее время |
| 6 | Подсистема периодического тестирования СЗИ НСД | | - проведение периодического тестирования функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест - программ, имитирующих попытки НСД |
| 7 | Подсистема наличия средств восстановления СЗИ НСД | | - наличие средств восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности |
| 8 | Подсистема антивирусной защиты информации | | * генерация данных аудита * ассоциация идентификатора пользователя * просмотр аудита * ограниченный просмотр аудита * выборочный просмотр аудита * управление режимом выполнения функций безопасности * управление данными ФБО * роли безопасности * базовое обнаружение КВ * проверка файлов, полученных по каналам передачи данных * методы анализа * выполнение проверок * запуск выполнения проверок внешней программой   - удаление КВ  - обновление БД ПКВ |
| 9 | Подсистема межсетевой защиты | | * сигналы нарушения безопасности * генерация данных аудита * просмотр аудита * избирательный аудит * аутентификация до любых действий пользователя * идентификация до любых действий пользователя * полное управление информационными потоками * простые атрибуты безопасности * управление режимом выполнения функций безопасности * управление данными функций безопасности * спецификация функций управления * роли безопасности * управление атрибутами безопасности * ручное восстановление * тестирование функциональных возможностей безопасности |

### **Требования к способам и средствам связи для информационного обмена между компонентами системы**

Информационный обмен между компонентами СЗПДн АС «Pharmacy» должен осуществляться с использованием существующих каналов и средств связи Заказчика. Способ и средства связи для информационного обмена между компонентами системы могут быть уточнены на этапе разработки Технического проекта.

### **Требования к характеристикам взаимосвязей создаваемой системы со смежными системами**

СЗПДн АС «Pharmacy» должна взаимодействовать с подсистемами АС Организации, используя существующие механизмы связи и протоколы взаимодействия, которые должны быть уточнены в Техническом проекте.

### **Требования к режимам функционирования системы**

СЗПДн АС «Pharmacy» должна поддерживать функционирование в следующих режимах:

* + - * основной;
      * режим проведения технологических работ;
      * аварийный режим.

### **Перспективы развития и модернизации системы**

СЗПДн АС «Pharmacy» должна создаваться с учетом возможностей ее расширения при увеличении числа рабочих мест пользователей, серверов и активного сетевого оборудования АС «Pharmacy».

## **Требования по стандартизации и унификации**

При создании СЗПДн АС «Pharmacy» должны соблюдаться требования нормативных документов в области информатизации и защиты информации законодательства Российской Федерации.

Применяемые для построения СЗПДн АС «Pharmacy» СрЗИ должны быть сертифицированы в системе сертификации средств защиты информации по требованиям безопасности информации ФСТЭК России или ФСБ России.

## **Требования к численности и квалификации персонала системы и режиму его работы**

На этапе разработки Технического проекта должны быть определены следующие решения по обслуживающему персоналу СЗПДн АС «Pharmacy»:

* решения по квалификации обслуживающего персонала с указанием необходимых курсов повышения квалификации;
* решения по распределению ответственности персонала по обслуживанию СЗПДн АС «Pharmacy».

## **Требования к показателям назначения системы**

СЗПДн АС «Pharmacy» должна обеспечивать защиту ПДн, обрабатываемых в АС Организации, от угроз безопасности ПДн, приведенных в Модели угроз безопасности ПДн, и соответствовать требованиям законодательства Российской Федерации по защите ПДн.

Выполнение указанных показателей назначения СЗПДн АС «Pharmacy» проверяется на этапе Приемочных испытаний СЗПДн АС «Pharmacy».

## **Требования к надежности**

Надежность и оперативная готовность СЗПДн АС «Pharmacy» должна обеспечиваться выполнением следующих требований:

* возможность непрерывной работы с учетом перерывов, необходимых для технического обслуживания;
* оперативное восстановление данных и работоспособности оборудования СЗПДн АС «Pharmacy» в случаях выхода из строя оборудования и при чрезвычайных ситуациях. Допустимыми способами оперативного восстановления являются (но не исчерпываются):
  + наличие резервных копий файлов конфигурации компонентов СЗПДн АС «Pharmacy»
  + использование технологии виртуализации серверов;
  + применение избыточности в аппаратных компонентах СЗПДн АС «Pharmacy»

## **Требования к эксплуатации, техническому обслуживанию, ремонту и хранению элементов системы**

Эксплуатация и техническое обслуживание компонентов СЗПДн АС «Pharmacy» должны проводиться в соответствии с эксплуатационной документацией компонентов СЗПДн АС «Pharmacy» и документами, создаваемыми на стадии Рабочей документации.

Размещение (хранение) компонентов СЗПДн АС «Pharmacy» должно осуществляться в специализированных помещениях, требования к которым определяются в Техническом проекте. Состав требований должен включать:

* требования по размещению (наличию специализированных помещений, стоек, свободного места в стойках);
* требования по физической безопасности (системы пожарной безопасности, видеонаблюдения, контроля и управления доступом в помещения);
* требования по электропитанию (величина запаса по мощности электропитания помещения);
* требования по кондиционированию и вентиляции (наличие системы охлаждения и величина запаса мощности по холоду);
* требования к каналам передачи данных (наличие портов, пропускная способность);
* требования к виртуальной инфраструктуре (количество поддерживаемых процессоров, оперативной памяти).

## **Требования к функциям, выполняемым системой**

Для реализации функций СЗПДн АС «Pharmacy» должны использоваться:

* встроенные СрЗИ - возможности и механизмы защиты информации, предоставляемые операционной системой (ОС), СУБД, прикладным ПО, телекоммуникационным и сетевым оборудованием, сертифицированные по требованиям безопасности информации Российской Федерации;
* организационные мероприятия по защите ПДн.

Для определения конкретных требований к функциям СЗПДн, из множества угроз (определенных в модели угроз) выделяются компоненты (уязвимости, способы реализации угроз, деструктивные действия, источники, каналы утечки), на нейтрализацию которых будут направлены требования.

Условные обозначения угроз и элементов угроз приведены в Модели угроз АС «Pharmacy».

Условные обозначения требований безопасности ПДн приведены в "Составе и содержании организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных" (утверждены приказом ФСТЭК России №21 от 18 февраля 2013 года).

## **Требования к видам обеспечения**

При создании СЗПДн АС «Pharmacy» должны выполняться требования к следующим видам обеспечения:

* + - техническое обеспечение;
    - программное обеспечение;
    - методическое и организационное обеспечение.

### **Требования к техническому обеспечению**

В качестве производителей технических средств, применяемых для создания СЗПДн АС «Pharmacy» должны рассматриваться производители технических средств АС "Pharmacy".

Технические средства СЗПДн АС «Pharmacy» должны снабжаться сервисными контрактами сроком не менее 2-х лет.

### **Требования к программному обеспечению**

Специальное ПО СЗПДн АС «Pharmacy» и его компоненты, устанавливаемые на компьютеры АС «Pharmacy», должны функционировать в среде используемых на них ОС.

Специальное ПО СЗПДн АС «Pharmacy» должно обеспечивать возможность адаптации к изменению конфигурации компьютеров, в том числе к введению нового оборудования АС «Pharmacy»

Все ПО СЗПДн АС «Pharmacy» должно поставляться с комплектами соответствующих лицензий на его использование и контрактами технической поддержки сроком не менее 2-х лет.

Программные компоненты СЗПДн АС «Pharmacy» могут функционировать в виртуализированной инфраструктуре, требования к которой определяются на этапе разработки Технического проекта.

### **Требования к методическому и другим видам обеспечения**

Методическое и организационное обеспечение СЗПДн АС «Pharmacy» должно соответствовать требованиям руководящих и нормативных документов ФСТЭК России и ФСБ России и включать комплект необходимой организационно-распорядительной документации (ОРД) в части защиты ПДн.

## **Состав и содержание работ по созданию системы**

Стадии и этапы работ по созданию АС «Pharmacy», а также содержание и результаты этих работ представлены в таблице.

Таблица 5 – Содержание и результаты работ по созданию АС

|  |  |  |  |
| --- | --- | --- | --- |
| Стадия | Этап работы | Организации -исполнители работ | Состав и результаты работ |
| Проектирование АС | Построение модели угроз и нарушителя  безопасности информации | Исполнитель | Модель угроз и нарушителя  безопасности информации объекта АС «Pharmacy» |
| Разработка ТЗ на создание АС «Pharmacy» | ТЗ на создание АС «Pharmacy» |
| Разработка ОРД по защите ПДн | ОРД по защите ПДн в АС «Pharmacy» |
| Ввод в действие | Подготовка персонала | Заказчик | Обучение персонала АС «Pharmacy» Проверка способности персонала обеспечивать функционирование АС «Pharmacy». |
| Опытная эксплуатация АС «Pharmacy» | Исполнитель совместно с Заказчиком | Опытная эксплуатация АС «Pharmacy» в соответствии с Программой опытной эксплуатации. Анализ, доработка, наладка компонентов АС «Pharmacy» (при необходимости) |
| Сопровождение | Гарантийное обслуживание АС «Pharmacy» Послегарантийное обслуживание АС «Pharmacy» | Исполнитель совместно с Заказчиком | Выполнение работ в соответствии с гарантийными обязательствами на АС «Pharmacy» .Выполнение послегарантийного обслуживания АС «Pharmacy». |

## **Порядок контроля и приемки системы**

Испытания Системы должны быть организованы и проведены в соответствии с ГОСТ 34.603-92 «Информационная технология. Виды испытаний автоматизированных систем».

Предусматриваются следующие виды испытаний:

* Предварительные испытания;
* Приемочные испытания;
* Опытная эксплуатация;

Объем, виды и методы испытаний определяются соответствующими программами и методиками в составе проектной и рабочей документации.

Результаты проведения испытаний должны быть зафиксированы в актах испытаний и протоколах испытаний. Положительные результаты испытаний, зафиксированные этими актами и протоколами, являются основанием для подписания актов сдачи-приемки выполненных работ соответствующего этапа развития Системы.

Состав участников (Комиссия), место проведения работ, а также сроки проведения работ по приемке Системы должны определяться и утверждаться распоряжением генеральным директором ООО «Ромашка».

По результатам приемки подписывается акт приемочной комиссии.

Все обнаруженные недостатки в функционировании и в документации Системы, выявленные в процессе испытаний, фиксируются Комиссией и устраняются Исполнителем.

## **Требования к составу и содержанию работ по подготовке объекта автоматизации к вводу системы в действие.**

При подготовке к вводу в действие СЗПДн АС «Pharmacy» Организация, осуществляющая ввод действие, должна подготовить и согласовать с Заказчиком список технических средств, доступ к которым должен быть предоставлен для проведения работ по вводу в действие СЗПДн АС «Pharmacy».

При подготовке к вводу в действие СЗПДн АС «Pharmacy» Заказчик должен обеспечить:

* предоставление доступа к компонентам АС «Pharmacy» сотрудникам Организации, осуществляющей ввод действие;
* предоставление технических средств и требуемых им ресурсов в соответствии с требованиями.
* готовность инфраструктуры к установке компонентов СЗПДн АС «Pharmacy».
* наличие обученного персонала для обеспечения эксплуатации компонентов СЗПДн АС «Pharmacy».
* утверждение ОРД, созданной на этапе разработки ОРД по защите ПДн;
* издание приказов о формировании соответствующих приемочных комиссий по вводу в действие СЗПДн АС «Pharmacy».

1. **Требования к документам.**
2. Аналитический отчет об обследовании процессов обработки ПДн;
3. Модель УБПДн;

3.ТЗ на создание СЗПДн АС «Pharmacy»;

4. ОРД по защите ПДн;

1. Технический проект, в составе;
2. Рабочая документация;
3. Эксплуатационная документация, в составе;
4. Подготовка к предварительным испытаниям;
5. **Источники разработки.**

ГОСТ 34.201-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем»;

ГОСТ 24.601-86 «Единая система стандартов автоматизированных систем управления. Автоматизированные системы. Стадии создания»;

Федеральный закон от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации».

Федеральный от 27 июля 2006 г. №152-ФЗ закон «О персональных данных».

РД Автоматизированные системы «Защита от несанкционированного доступа к информации  
Классификация автоматизированных систем и требования по защите информации» (утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.)

Федеральная служба по техническому и экспортному контролю (ФСТЭК России) Информационное сообщение «Об утверждении требований к средствам антивирусной защиты» от 30 июля 2012 г. N 240/24/3095

Федеральная служба по техническому и экспортному контролю Информационное сообщение «Об утверждении требований к межсетевым экранам» От 28 апреля 2016 г. N 240/24/1986

Документы по сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации

Методический документ профиль защиты средств антивирусной защиты типа «Б» пятого класса защиты ИТ.САВЗ.Б5.ПЗ

Методический документ профиль защиты межсетевых экранов типа «Б» пятого класса защиты ИТ.МЭ.Б5.ПЗ

Федеральная служба по техническому и экспортному контролю Информационное сообщение «Об утверждении требований к межсетевым экранам» От 28 апреля 2016 г. N 240/24/1986

Федеральная служба по техническому и экспортному контролю (ФСТЭК России) Информационное письмо «Об утверждении требований к системам обнаружения вторжений»

РД Гостехкомиссии России «Защита от несанкционированного доступа к информации. Термины и определения».

РД Гостехкомиссии России «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации».

РД Гостехкомиссии России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (1992 г.).

РД 50-34.698-90 «Методические указания. Информационная технология. Комплекс Стандартов и руководящих документов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов».

Нормативный документ ФСТЭК России «Базовая модель угроз безопасности персональных данных при их обработке, в информационных системах персональных данных» (утверждена 15 февраля 2008г. заместителем директора ФСТЭК России).

Нормативный документ ФСБ России «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации» (ФСБ России, № 149/5-144, 2008).

Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденное приказом ФСБ России от 9 февраля 2005 года № 66 (зарегистрирован Минюстом России 3 марта 2005 года, регистрационный № 6382)