

УТВЕРЖДАЮ

Главный врач УЗ «35-я городская клиническая
поликлиника»

г. Минска

А. Н. Линдеров

« 21 » 05 2024г.



ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ

к проектированию системы защиты информации информационной системы
учреждения здравоохранения
«35-я городская клиническая поликлиника»

1. Общие сведения

Настоящий документ содержит требования к проектированию системы защиты информации (далее – СЗИ) информационной системы (далее – ИС) Учреждения здравоохранения «35-я городская клиническая поликлиника» (далее – Учреждение), в соответствии с Положением о порядке технической и криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, утвержденным приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 66 «О мерах реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449» в редакции приказа Оперативно-аналитического центра при Президенте Республики Беларусь от 12 ноября 2021 № 195 «О технической и криптографической защите персональных данных» (далее – Приказ № 66).

ИС Учреждения включает:

- локальную вычислительную сеть (далее – ЛВС);
- физических серверов – 2 шт.;
- виртуальных серверов – 3 шт.;
- количество эксплуатируемых информационных систем – 1 шт.;
- автоматизированные рабочие места пользователей - ориентировочно – 167 шт.;

Адрес местонахождения Учреждения: Республика Беларусь, г. Минск, ул. Серова, д.15

2. Перечень выполняемых работ

Проектирование СЗИ ИС Учреждения включает следующие работы:

- 2.1 Обследование ИС Учреждения;
- 2.2 Разработка (корректировка существующей) Политики информационной безопасности Учреждения;
- 2.3 Разработка недостающих локальных правовых актов (далее ЛПА) Учреждения в области информационной безопасности (далее – ИБ);
- 2.4 Разработка технического задания на создание СЗИ ИС Учреждения (далее – техническое задание);
- 2.5 Выбор средств технической и криптографической защиты информации, удовлетворяющих требованиям технического задания;
- 2.6 Разработка общей схемы СЗИ.
- 2.7 Разработка спецификации средств технической и криптографической защиты информации.

3. Требования к выполнению работ

3.1 Работы по обследованию ИС Учреждения включают:

- анализ организационной структуры и ИТ-инфраструктуры Учреждения, определение состава, границ и мест размещения элементов информационных систем (аппаратных и программных);
- инвентаризацию активов ЛВС Учреждения;
- анализ взаимодействия информационных систем, входящих в состав ИС Учреждения и их элементов;
- анализ информационных потоков ИС Учреждения;
- определение и анализ физических и логических границ ИС Учреждения;
- анализ соблюдения требований Приказа № 66 к СЗИ ИС Учреждения зависимости от классов типовых ИС;
- анализ ЛПА Учреждения, регламентирующих вопросы ИБ, с целью оценки их соответствия требованиям законодательства Республики Беларусь в области защиты информации и Приказа № 66;
- анализ следующих процессов обеспечения ИБ:
 - разграничение доступа пользователей к объектам информационных систем;
 - резервирование и уничтожение информации;
 - защита от вредоносного программного обеспечения;
 - использование съемных носителей информации;
 - использование электронной почты;
 - парольная политика
 - обновление средств защиты информации;
 - осуществление контроля (мониторинга) за функционированием информационных систем и системы защиты информации;
 - реагирование на события ИБ и ликвидация их последствий;
 - управление криптографическими ключами, в том числе их генерацией, распределением, хранением, доступом к ним и их уничтожению;
 - обучение (повышение квалификации) пользователей ИС.

По результатам обследования ИС Учреждения должен быть разработан отчет, содержащий следующие сведения:

- рекомендации с обоснованием по отнесению ИС Учреждения к классам типовых ИС в соответствии с Положением о порядке технической и криптографической защиты информации в информационных системах, распространение и (или) предоставление которой ограничено, утвержденным Приказом № 66;
- отчет о соответствии (несоответствии) СЗИ ИС и ЛПА Учреждения требованиям законодательства Республики Беларусь в области защиты информации и Приказа № 66 в зависимости от классов типовых ИС;
- предложения (рекомендации) по совершенствованию системы защиты информации Учреждения.

3.2 Политика информационной безопасности Учреждения, Техническое задание, Общая схема СЗИ должны быть разработаны в соответствии с требованиями Приказа № 66.

3.3 Проекты недостающих (несоответствующих) ЛПА Учреждения должны быть разработаны с учетом предложений (рекомендаций), изложенных в отчете об обследовании.

4. Требования к отчётной документации

Отчетные документы должны быть представлены в одном экземпляре на бумажном носителе и в одном экземпляре в электронном виде на CD - диске. Электронное представление документов должно соответствовать формату редакторов Microsoft Word.

5. Требования к срокам выполнения работ

Срок выполнения работ по проектированию СЗИ ИС Учреждения – не более 50 (пятьдесят) рабочих дней с даты подписания Договора обеими сторонами.

6. Требования к сдаче-приемке работ

6.1. По окончании выполнения работ Учреждению должен быть предоставлен акт сдачи-приёмки выполненных работ (далее – Акт).

6.2. По требованию руководства Учреждения должна быть проведена защита проекта СЗИ ИС.

6.3. Учреждение в течение 5 (Пять) рабочих дней после получения Акта должно осуществить приёмку выполненных работ и подписать Акт, либо предоставить мотивированный отказ от его подписания.

7. Условия оплаты работ

Оплата выполненных работ осуществляется в течение 10 (десяти) банковских дней с даты подписания Акта.

8. Квалификационные требования к исполнителю

К исполнителю предъявляются следующие требования:

- наличие лицензии Оперативно-аналитического центра при Президенте Республики Беларусь на право осуществления деятельности по технической и (или) криптографической защите информации (проектирование, создание, аттестация систем защиты информации информационных систем, предназначенных для обработки информации, распространение и(или) предоставление которой ограничено, не отнесенной к государственным секретам);
- наличие сертифицированной системы менеджмента информационной безопасности на соответствие требованиям СТБ ISO/IEC 27001:2016 применительно к проектированию, созданию и аттестации систем защиты информации информационных систем и (или) наличие сертифицированной системы менеджмента качества в соответствии с требованиями СТБ ISO 9001:2015 применительно к проектированию, созданию и аттестации систем защиты информации информационных систем;
- документально подтвержденный положительный опыт выполнения работ по проектированию СЗИ ИС в государственных учреждениях (предприятиях) (не менее 3 (трех) отзывов).

Разработано:

Ведущий инженер-электроник



С.А. Дунькович

Согласованно:

Ведущий экономист



Е.А. Панченко