ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ЗДРАВООХРАНЕНИЯ

«БЕЛОВОДСКАЯ ЦЕНТРАЛЬНАЯ РАЙОННАЯ МНОГОПРОФИЛЬНАЯ БОЛЬНИЦА» ЛУГАНСКОЙ НАРОДНОЙ РЕСПУБЛИКИ

(ГБУЗ «БВЦРМБ» ЛНР)

ПРИКАЗ № 42

пгт. Беловодск «03» 03 2025г.

Об утверждении Плана защиты автоматизированной системы Государственного бюджетного учреждения здравоохранения «Беловодская центральная районная многопрофильная больница» Луганской Народной Республики от несанкционированного доступа к информации и незаконного вмешательства в процесс ее функционирования

В целях организации и проведения работ по обеспечению антитеррористической защищенности, охраны жизни, здоровья пациентов и сотрудников Государственного бюджетного учреждения здравоохранения «Беловодская центральная районная многопрофильная больница» Луганской Народной Республики (ГБУЗ «БВЦРМБ» ЛНР), а также в соответствии с требованиями Федерального закона от 26.07.2017г. №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

ПРИКАЗЫВАЮ:

1. Утвердить и ввести в действие с 01 января 2025г.:

План защиты автоматизированной системы Государственного бюджетного учреждения здравоохранения «Беловодская центральная районная многопрофильная больница» Луганской Народной Республики от несанкционированного доступа к информации и незаконного вмешательства в процесс ее функционирования .

2. Возложить ответственность за исполнение настоящего Приказа и Плана защиты на инженера-программиста и юрисконсульта учреждения здравоохранения.

3. Секретарю руководителя ознакомить всех руководителей/заведующих структурных и обособленных подразделений учреждения здравоохранения.

4. Контроль за исполнением настоящего приказа оставляю за собой.

Главный врач Г.В. Михалёв

УТВЕРЖДАЮ

Главный врач ГБУЗ «Беловодская центральная районная многопрофильная больница» Луганской Народной Республики

_____Михалёв Г.В.

«03» марта 2025 г.

ПЛАН ЗАЩИТЫ

автоматизированной системы Государственного бюджетного учреждения здравоохранения «Беловодская центральная многопрофильная больница» Луганской Народной Республики от несанкционированного доступа к информации и незаконного вмешательства в процесс ее функционирования

2025 г.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий документ определяет комплекс организационно-технических мер по защите автоматизированной системы (в дальнейшем по тексту - АС) Государственного бюджетного учреждения здравоохранения «Беловодская центральная районная многопрофильная больница» Луганской Народной Республики (в дальнейшем по тексту – ГБУЗ «БВЦРМБ»ЛНР) от несанкционированного доступа (в дальнейшем по тексту - НСД) к циркулирующей в ней информации, а также незаконного вмешательства в процесс ее функционирования.

1.2. Документ не регламентирует вопросы охраны помещений и обеспечения сохранности и физической целостности компонентов АС, защиты от стихийных бедствий (пожаров, наводнений), сбоев и отказов технических средств, сбоев в системе энергоснабжения и вопросы восстановления данных, а также меры обеспечения личной безопасности персонала.

1.3. Требования настоящего документа распространяются на все структурные и обособленные подразделения ГБУЗ «БВЦРМБ» ЛНР, в которых осуществляется автоматизированная обработка подлежащей защите информации, а также подразделения, осуществляющие сопровождение, обслуживание и обеспечение нормального функционирования АС.

2. ЦЕЛЬ И ЗАДАЧИ ЗАЩИТЫ

2.1. Основной целью, на достижение которой направлены все положения данного документа, является защита ГБУЗ «БВЦРМБ» ЛНР, ее клиентов и корреспондентов от возможного нанесения им ощутимого материального, морального или другого ущерба посредством случайного или преднамеренного несанкционированного вмешательства в процесс функционирования АС или несанкционированного доступа к циркулирующей в ней информации и ее незаконного использования.

2.2. Указанная цель достигается посредством обеспечения и постоянного поддержания следующих свойств информации и автоматизированной системы ее обработки:

- доступности обрабатываемой информации (устойчивого функционирования АС, при котором пользователи системы имеют возможность получения необходимой им информации и результатов решения задач за приемлемое время);

• конфиденциальности определенной части информации, хранимой, обрабатываемой и передаваемой по каналам связи;

• целостности информации, хранимой и обрабатываемой в АС и передаваемой по каналам связи.

2.3. Для достижения основной цели защиты и обеспечения указанных свойств АС и циркулирующей в ней информации система безопасности АС должна обеспечивать эффективное решение следующих задач:

• защиту АС от вмешательства в процесс ее функционирования посторонних лиц (возможность использования автоматизированной подсистемы и доступ к ее ресурсам должны иметь только зарегистрированные установленным порядком пользователи - сотрудники структурных подразделений);

• разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам АС (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям АС для выполнения своих служебных обязанностей);

• защиту хранимых и передаваемых по каналам связи данных от несанкционированной модификации (искажения), фальсификации, уничтожения и подтверждение аутентичности (авторства) электронных документов;

• защиту информации ограниченного распространения, хранимой, обрабатываемой и передаваемой по каналам связи, от несанкционированного разглашения (утечки);

• защиту от несанкционированной модификации (подмены, уничтожения) и контроль целостности используемых в АС программных средств, а также защиту системы от внедрения несанкционированных программ, включая компьютерные вирусы;

• контроль целостности операционной среды исполнения прикладных программ (решения прикладных задач) и ее восстановление в случае нарушения.

3. МЕРЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Поставленная основная цель защиты и решение перечисленных задач достигается:

• строгой регламентацией процессов обработки данных с применением средств автоматизации и действий сотрудников ГБУЗ «БВЦРМБ» ЛНР, использующих АС, а также действий персонала, осуществляющего

обслуживание и модификацию программных и технических средств АС, на основе утвержденных руководством учреждения организационно-распорядительных документов по вопросам обеспечения информационной безопасности;

- полнотой охвата всех аспектов проблемы, непротиворечивостью (согласованностью) и реальной выполнимостью требований организационно-распорядительных документов по вопросам обеспечения информационной безопасности в АС;
- назначением и подготовкой должностных лиц (сотрудников), ответственных за организацию и осуществление практических мероприятий по обеспечению безопасности информации и процессов ее обработки;
- наделением каждого сотрудника учреждения (пользователя) минимально необходимыми для выполнения им своих функциональных обязанностей полномочиями по доступу к ресурсам АС;
- четким знанием и строгим соблюдением всеми сотрудниками, использующими и обслуживающими аппаратные и программные средства АС, установленных требований по вопросам обеспечения безопасности информации;
- персональной ответственностью каждого сотрудника, участвующего в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющего доступ к ресурсам АС за свои действия;
- строгим учетом всех подлежащих защите ресурсов системы (информации, задач, каналов, рабочих станций, серверов и т.д.);
- принятием эффективных мер обеспечения физической целостности технических средств и непрерывным поддержанием необходимого уровня защищенности компонентов АС;
- применением физических и технических (программно-аппаратных) средств защиты ресурсов системы и непрерывной административной поддержкой их использования;
- проведением работы с персоналом (подбор, разъяснение, обучение и т.п.) и эффективным контролем за соблюдением сотрудниками - пользователями АС требований по обеспечению информационной безопасности;
- юридической защитой интересов учреждения при взаимодействии с внешними организациями (связанном с обменом информацией) от противоправных действий как со стороны этих организаций, так и от несанкционированных действий обслуживающего персонала и третьих лиц;

• проведением постоянного анализа эффективности и достаточности принятых мер и применяемых средств защиты информации, разработкой и реализацией предложений по совершенствованию системы защиты АС.

4. ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АС (ОСНОВНЫЕ ПОЛОЖЕНИЯ ПОЛИТИКИ БЕЗОПАСНОСТИ)

4.1. Организационные, технологические и технические мероприятия по защите информации в АС ГБУЗ «БВЦРМБ» ЛНР должны проводиться в соответствии с требованиям действующего законодательства, а также нормативно - методическими материалами и организационно - распорядительными документами по вопросам обеспечения информационной безопасности в автоматизированных системах.

4.2. Все ресурсы АС должны быть установленным порядком категорированы (для каждого ресурса должен быть определен требуемый уровень защищенности). Подлежащие защите ресурсы системы (информация, задачи, программы, рабочие станции, сервера и т.д.) подлежат строгому учету (на основе использования соответствующих формуляров или специализированных баз данных).

4.3. На всех рабочих станциях (РС) АС, подлежащих защите, должны быть установлены необходимые технические средства защиты (соответствующие требуемому уровню защищенности - категории РС).

4.4. Все сотрудники учреждения, использующие при работе АС, должны быть ознакомлены с Планом защиты АС в части, их касающейся, должны знать и неукоснительно выполнять технологические инструкции и “Общие обязанности сотрудников по обеспечению безопасности информации при использовании АС”. Доведение требований до лиц, допущенных к обработке защищаемой информации, должно осуществляться начальниками подразделений под роспись.

Сотрудники учреждения, допущенные к работе с АС, должны нести персональную ответственность за нарушение установленного порядка автоматизированной обработки информации, правил хранения, использования и передачи находящихся в их распоряжении защищаемых ресурсов системы. Каждый сотрудник (при приеме на работу или при допуске к работе с защищаемыми ресурсами АС) доложен подписывать Соглашение-обязательство о соблюдении и ответственности за нарушение установленных требований по сохранению банковской, служебной и коммерческой тайны, а также правил работы с защищаемой информацией в АС. Любое грубое нарушение порядка и правил работы в АС сотрудниками должно расследоваться. К виновным должны применяться адекватные меры воздействия. Мера ответственности

персонала за действия, совершенные в нарушение установленных правил обеспечения безопасной автоматизированной обработки информации, определяется нанесенным ущербом, наличием злого умысла и другими факторами по усмотрению руководства учреждения .

4.5. Допуск сотрудников к работе с автоматизированной подсистемой и доступ к ее ресурсам должен быть строго регламентирован. Любые изменения состава и полномочий пользователей АС должны производиться установленным порядком. Каждому сотруднику ГБУЗ «БВЦРМБ» ЛНР (пользователю) должны предоставляться минимально необходимые для выполнения им своих функциональных обязанностей права и полномочия по доступу к ресурсам АС (производственная необходимость предоставления сотрудникам полномочий и прав доступа к ресурсам АС определяется руководством соответствующих структурных подразделений). Ни один сотрудник не должен обладать всей полнотой полномочий для единоличного бесконтрольного уничтожения, изменения либо создания и авторизации ресурсов в АС. Руководители структурных подразделений обязаны своевременно предоставлять заявки на предоставление своим сотрудникам или лишение (в случае увольнения, перевода, болезни и т.п.) сотрудников соответствующих прав доступа и полномочий по работе с ресурсами АС.

4.6. Аппаратно-программная конфигурация рабочих станций (автоматизированных рабочих мест), на которых обрабатывается защищаемая информация (с которых возможен доступ к защищаемым ресурсам), должна соответствовать кругу возложенных на пользователей данной РС функциональных обязанностей. Все неиспользуемые в работе (лишние) устройства ввода-вывода информации (USB, COM, LPT порты, дисководы DVD-CD) на таких РС должны быть отключены (удалены физически или логически), не нужные для работы программные средства и данные с дисков РС должны быть удалены.

Для упрощения сопровождения, обслуживания и организации защиты РС должны оснащаться программными средствами и конфигурироваться унифицировано (в соответствии с установленными правилами).

4.7. Ввод в эксплуатацию новых РС и все изменения в конфигурации технических и программных средств существующих РС в АС должны осуществляться только установленным порядком.

4.8. Эксплуатация подлежащих защите РС должна осуществляться в помещениях, оборудованных автоматическими замками, средствами сигнализации и постоянно находящимися под охраной или наблюдением, исключающим возможность бесконтрольного проникновения в помещения посторонних лиц и обеспечивающим физическую сохранность находящихся в помещении защищаемых ресурсов (РС, документов, реквизитов доступа и т.п.).

Размещение и установка технических средств ПЭВМ таких РС (АРМ) должна исключать возможность визуального просмотра вводимой (выводимой) информации лицами, не имеющими к ней отношения.

В помещениях во время обработки и отображения на ПЭВМ конфиденциальной информации должны присутствовать только лица, допущенные к работе с данной информацией. Организация приема посетителей должна исключать возможность их визуального ознакомления с защищаемой информацией, к которой они не допущены.

По окончании рабочего дня помещения с установленными защищенными РС должны сдаваться под охрану, с включением сигнализации.

4. ПОРЯДОК ПЕРЕСМОТРА ПЛАНА ЗАЩИТЫ

5.1. План защиты подлежит ***частичному*** пересмотру в следующих случаях:

- при изменении конфигурации, добавлении или удалении программных и технических средств в АС, не изменяющих технологию обработки информации;
- при изменении конфигурации и настроек технических средств защиты, используемых в АС;
- при изменении состава и обязанностей должностных лиц - пользователей и обслуживающего персонала АС и сотрудников, отвечающих за информационную безопасность в автоматизированной системе.

5.2. ***Профилактический*** пересмотр Плана защиты производится не реже 1 раза в год и имеет целью проверку соответствия определенных данным планом мер реальным условиям применения АПС и текущим требованиям к ее защите.

5.3. План защиты подлежит ***полному*** пересмотру в случае изменения технологии обработки информации или использовании новых технических средств защиты.

5.4. В случае частичного пересмотра могут быть добавлены, удалены или изменены различные приложения к Плану защиты АС.

5.5. Изменения, вносимые в план, не должны противоречить другим положениям Плана защиты и должны быть проверены на корректность, полноту и реальную выполнимость.

5.6. Любой пересмотр Плана защиты должен осуществляться с обязательным участием представителей Службы информационной безопасности ГБУЗ «БВЦРМБ» ЛНР.

6. ОТВЕТСТВЕННЫЕ ЗА РЕАЛИЗАЦИЮ ПЛАНА ЗАЩИТЫ

6.1. Ответственность за реализацию и соблюдение требований данного документа сотрудниками, допущенными к работе с АС, возлагается на начальников структурных подразделений и администраторов информационной безопасности (ответственных за информационную безопасность в подразделениях и на технологических участках).

6.2. За реализацию положений Плана защиты, связанных с применением и администрированием технических средств защиты информации от НСД отвечают ответственные за информационную безопасность в подразделениях и на технологических участках.

6.3. Реализация положений Плана защиты, связанных с сопровождением программного обеспечения и обслуживания технических средств, возлагается на уполномоченных сотрудников отдела ИТ.

6.4. Методическое руководство и контроль за выполнением требований настоящего документа возлагается на ответственных за информационную безопасность в подразделениях и на технологических участках.

7. ОСНОВНЫЕ ПОНЯТИЯ И ОПРЕДЕЛЕНИЯ

Под ***автоматизированной системой*** (АС) понимается организационно-техническая система, представляющая собой совокупность следующих взаимосвязанных компонентов:

- технических средств обработки и передачи данных (средств вычислительной техники и связи);
- методов и алгоритмов обработки данных в виде соответствующего программного обеспечения;
- информации (массивов, наборов, баз данных) на различных носителях;
- персонала,

объединенных по организационно-структурному, тематическому, технологическому или другим признакам для выполнения автоматизированной обработки информации (данных) с целью удовлетворения информационных потребностей государственных органов, государственных, общественных или коммерческих организаций и предприятий (юридических лиц), отдельных граждан (физических лиц) и иных участников процесса информационного взаимодействия.

Безопасность информации - такое состояние информации (информационных ресурсов) и автоматизированной системы ее обработки, при котором с требуемой надежностью обеспечивается защита информации (данных, ключей шифрования и

т.д.) от утечки, хищения, утраты, несанкционированного уничтожения, модификации (подделки), несанкционированного копирования, блокирования и т.п.

Для защиты информации в любой АС (подсистемы АС) требуется создание специальной ***системы безопасности (системы защиты)***, представляющей собой совокупность специального персонала, организационных мер и мероприятий, а также физических и технических средств защиты, применяемых в соответствии с общим замыслом.

Набор правил, регламентирующих функционирование АС в соответствии с необходимыми условиями обеспечения информационной безопасности, а так же действий персонала АС в случае нарушения этих условий, называется ***политикой безопасности.***

План защиты **-** документ, содержащий общее описание политики безопасности АС (подсистемы АС).

Юрисконсульт Я.Н. Луганская

Инженер-программист О.А. Иванов