УТВЕРЖДЕНА
Приказом ГУЗ «ГОККВД»
от «___»_____2025 №___

ГОСУДАРСТВЕННОЕ УЧРЕЖДЕНИЕ ЗДРАВООХРАНЕНИЯ «ГРОДНЕНСКИЙ ОБЛАСТНОЙ КЛИНИЧЕСКИЙ КОЖНО-ВЕНЕРОЛОГИЧЕСКИЙ ДИСПАНСЕР»
ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Гродно
2025

ОГЛАВЛЕНИЕ

ГЛАВА 1
ОБЛАСТЬ ПРИМЕНЕНИЯ

1. Политика информационной безопасности государственного учреждения здравоохранения «Гродненский областной клинический кожно-венерологический диспансер» (далее – Политика) устанавливает цели и программу действий работников государственного учреждения здравоохранения «Гродненский областной клинический кожно-венерологический диспансер» (далее – Учреждение) при создании и эксплуатации средств защиты информации информационных систем Учреждения в соответствии с деятельностью, потребностями и требованиями законодательства Республики Беларусь по технической и криптографической защите информации.

2. Действие Политики распространяется на:

руководителей и специалистов Учреждения, организующих и обеспечивающих эксплуатацию информационных систем, а также участвующих в создании и эксплуатации СЗИ данных информационных систем;

персонал сторонних организаций, которые оказывают услуги Учреждению по разработке, обслуживанию или сопровождению прикладного программного обеспечения и средств вычислительной техники.

3. Политика распространяет свое действие на все информационные системы Учреждения. Наименование информационных систем, соответствующие классы типовых информационных систем, а также ответственный за обеспечение защиты информации представлены в приложении 1 к Политике.

4. Перечень средств вычислительной техники, относящейся к информационным системам Учреждения, представлен в приложении 2 к Политике.

ГЛАВА 2
ОБЩИЕ ПОЛОЖЕНИЯ

5. В соответствии с требованиями законодательства Республики Беларусь информация, распространение и (или) предоставление которой ограничено, не отнесенная к государственным секретам, должна обрабатываться в информационных системах с применением системы защиты информации, аттестованной в порядке, установленном ОАЦ [1].

6. Политика – это совокупность документированных правил, процедур и требований в области защиты информации, действующих в информационных системах.

7. Политика разработана с учетом требований законодательства Республики Беларусь по вопросам защиты информации и устанавливает общие намерения и направления деятельности по обеспечению конфиденциальности, целостности, сохранности, подлинности и доступности информации, обрабатываемой в информационных системах.

8. Документами по информационной безопасности, детализирующими положения Политики применительно к информационным системам, согласно требованиям ОАЦ [2], является документация на СЗИ, которая разрабатывается и оформляется в виде отдельных локальных правовых актов.

9. Реализация Политики должна осуществляться на основе принципа непрерывности и строгого соблюдения установленных ею правил.

Внесение изменений в Политику осуществляется на периодической и внеплановой основе.

В случае изменения действующего законодательства применение Политики до внесения в нее изменений и дополнений осуществляется в части, не противоречащей требованиям законодательства Республики Беларусь.

Внеплановое внесение изменений может производиться по результатам анализа инцидентов информационной безопасности, актуальности, достаточности и эффективности используемых мер обеспечения информационной безопасности, а также по результатам проведения внутренних аудитов информационной безопасности и других контрольных мероприятий.

10. Ответственным за внесение изменений в Политику является администратор информационной безопасности.

ГЛАВА 3
ЦЕЛИ И ПРИНЦИПЫ ЗАЩИТЫ ИНФОРМАЦИИ

11. Цели защиты информации в ИС Учреждения сформированы и направлены на снижение угроз информационной безопасности до приемлемого уровня, при котором обеспечивается целостность, доступность и конфиденциальность принимаемой, обрабатываемой, хранимой и передаваемой информации, а также защищенность самих информационных ресурсов и средств автоматизации от несанкционированного доступа к ним.

12. Основными целями защиты информации в ИС Учреждения являются:

обеспечение требований законодательства Республики Беларусь;

недопущение неправомерного доступа, уничтожения, модификации (изменения), копирования, распространения и (или) предоставления информации, блокирования правомерного доступа к информации, а также иных неправомерных действий;

обеспечение прав субъектов информационных отношений при создании, использовании и эксплуатации ИС и информационных сетей, использовании информационных технологий, а также при формировании и использовании информационных ресурсов;

сохранение и неразглашение информации о частной жизни физических лиц и персональных данных, содержащихся в ИС [1];

обеспечение непрерывности функционирования прикладного и системного ПО, технических средств и ресурсов, обеспечивающих работоспособность ИС, в которой обрабатывается информация, распространения и (или) предоставление которой ограничено.

13. Обеспечение достижения поставленных целей защиты информации строится на основе следующих принципов:

реализация требований законодательства Республики Беларусь в части информационной безопасности ИС и мер контроля их защищенности;

определение ответственности субъектов информационных отношений по обеспечению и соблюдению требований Политики, в том числе с использованием программных, программно-аппаратных средств технической и криптографической защиты информации, а также посредством принятия соответствующих внутренних нормативных и организационно-методических документов. В соответствии с этим принципом распределение прав и обязанностей работников должно строится таким образом, чтобы в случае любого нарушения круг виновных был четко известен или сведен к минимуму. Наличие должностных лиц, ответственных за информационную безопасность в Учреждении, а также работников, осуществляющих практическую работу по обеспечению защиты информации, должно быть определено организационно-штатной структурой Учреждения, приказами или должностными инструкциями;

минимизации привилегий. Пользователи должны иметь только те права доступа, которые необходимы им для выполнения служебных обязанностей;

планирование, реализация и контроль эффективности использования защитных мер и средств защиты информации, создание механизма оперативного реагирования на угрозы информационной безопасности;

недопустимости перехода в открытое состояние путем своевременного выявления и оценки причин, условий и характера угроз информационной безопасности и дальнейшего прогнозирования развития событий на основе мониторинга инцидентов информационной безопасности;

многоуровневой защиты. За средствами инженерно-физической защиты должны следовать программно-технические средства. Должна обеспечиваться идентификация и аутентификация пользователей, управление доступом, протоколирование и аудит событий безопасности;

простоты и управляемости. Должна обеспечиваться согласованность конфигурации разных компонентов. На СЗИ должна быть разработана документация [2];

всеобщей поддержки мер безопасности. Должна быть предусмотрена реализация программ по осведомленности и обучению работников Учреждения о возможных факторах рисков информационной безопасности и мерах противодействия.

14. В Учреждении подлежат реализации с последующей поддержкой следующие основные меры защиты информации:

правовые меры: исполнение требований законодательства Республики Беларусь;

организационные меры: регламентация обеспечения особого режима допуска на территории (в помещениях), где может быть осуществлен доступ к информации (материальным носителям информации), регламентация разграничения доступа к информации по кругу лиц и характеру информации, а также определение технологических процедур администрирования;

технические меры: использование средств технической и криптографической защиты информации, а также меры по контролю защищенности информации;

физические меры: воспрепятствование физическому проникновению посторонних лиц в помещения, в которых размещаются серверное оборудование и технические средства, используемые при администрировании ИС.

ГЛАВА 4
ПРАВА И ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЕЙ

15. Пользователи обладают правами и обязанностями при использовании ИС в пределах предоставленных им полномочий и (или) прав.

16. Пользователи имеют право:

использовать информационные и технические ресурсы при исполнении своих должностных обязанностей;

осуществлять подключение и использовать ресурсы в соответствии с предоставленными ему правами;

руководствоваться Политикой и иными ЛПА при работе с информационной системой;

в части своих компетенций вносить предложения по возможному развитию и модернизации СЗИ.

17. Пользователи обязаны:

знать и применять в соответствии со своими должностными обязанностями принципы защиты информации;

использовать только свой идентификатор и пароль для доступа к ресурсам ИС;

формировать пароли для доступа к ресурсам в соответствии с требованиями к сложности пароля;

исключать возможность ознакомления с персональным паролем посторонних лиц как при хранении, так и при его вводе;

в случае разглашения или компрометации пароля незамедлительно предпринять меры по его смене либо уведомить администратора информационной безопасности;

уведомить администратора информационной безопасности, если выявлены признаки вредоносного ПО;

соблюдать правила «чистого стола» и «чистого экрана»;

завершать сеанс связи по окончании работы, а также блокировать или выключать средство вычислительной техники при оставлении рабочего места, если иное не определено технологическим процессом;

предпринимать меры ограничения физического доступа к объектам ИС, на которых выполняется обработка информации ограниченного распространения, средствах защиты информации и объектам, на которых выполняется администрирование ИС.

18. Пользователи несут ответственность:

за распространение и (или) предоставление информации, обрабатываемой в ИС и ресурсах, пользователям, не имеющим права доступа;

за нарушение порядка доступа к информации, обрабатываемой в ИС;

за непринятие соответствующих мер по защите информации;

за невыполнение установленных правил, требований Политики и иных ЛПА Учреждения.

ГЛАВА 5
ПОРЯДОК ОРГАНИЗАЦИИ ВЗАИМОДЕЙСТВИЯ С ИНЫМИ ИС

19. Организация взаимодействия систем, осуществляющих обработку информации, распространение и (или) предоставление которой ограничено, с иными ИС осуществляется в соответствии с Требованиями к организации взаимодействия информационных систем, отраженными в приложении 4 к Положению о порядке технической и криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, утвержденному приказом ОАЦ от 20.02.2020 № 66, и строится на принципах соблюдения полноты, достоверности предоставляемой информации, получаемой, обрабатываемой и размещаемой в рамках межсистемного взаимодействия, а также конфиденциальности информации, доступ к которой ограничен законодательством об информации, информатизации и защите информации.

Взаимодействие с иными ИС осуществляется на основании регламента (или иного документа) информационного взаимодействия между ИС Учреждения и иными ИС.

ГЛАВА 6
КОНТРОЛЬ СОБЛЮДЕНИЯ ТРЕБОВАНИЙ ПОЛИТИКИ

20. Общее руководство обеспечением защиты информации, координацию работ и контроль исполнения мероприятий по информационной безопасности осуществляет руководитель Учреждения.

Текущий контроль соблюдения Политики возлагается на администратора информационной безопасности.

Контроль осуществляется путем проведения мониторинга и менеджмента инцидентов информационной безопасности, по результатам оценки информационной безопасности, а также в рамках иных контрольных мероприятий.

21. Наличие должностного лица, ответственного за осуществление защиты информации в ИС (администратор информационной безопасности), а также администратора, осуществляющего практическую работу по обеспечению защиты информации, должен быть определен организационно-штатной структурой Учреждения, приказами и должностными инструкциями работникам.

22. Ответственность за обеспечение безопасности информации и системы ее обработки должна быть возложена на каждого работника Учреждения в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей работников должно строиться таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.

ГЛАВА 7
ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ, ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

23. В Политике применяются следующие термины с соответствующими им определениями:

администратор информационной безопасности – специалист, назначенный в установленном порядке, ответственный за обеспечение безопасности информационной системы, реализацию и непрерывность соблюдения установленных административных мер защиты, осуществляющий постоянную организационную поддержку функционирования применяемых физических и технических средств защиты;

доступность – свойство, характеризующее возможности предоставлять необходимые ресурсы (вычислительные, коммуникационные, информационные, функциональные) авторизованным пользователям в требуемое им время;

доступ к информации – возможность получения информации и пользования ею;

защита информации – комплекс правовых, организационных и технических мер, направленных на обеспечение конфиденциальности, целостности, подлинности, доступности и сохранности информации;

идентификация − сравнение предъявляемого уникального имени (идентификатора) с перечнем присвоенных идентификаторов;

информационная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций;

инцидент информационной безопасности – событие, указывающее на свершившуюся, предпринимаемую или вероятную реализацию угрозы информационной безопасности, т.е. реализацию нарушения свойств информационной безопасности активов информационной системы;

конфиденциальность информации – требование не допускать распространения и (или) предоставления информации без согласия ее обладателя или иного основания, предусмотренного законодательными актами;

объект информационной системы – средства вычислительной техники, сетевое оборудование, системное и прикладное программное обеспечение, средства технической и криптографической защиты информации;

пользователь – субъект информационных отношений, получивший доступ к информационной системе;

система защиты информации – совокупность мер по защите информации, реализованных в информационной системе;

средства защиты информации – средства защиты государственных секретов, средства криптографической защиты информации, средства технической защиты информации;

средства криптографической защиты информации – программные, программно-аппаратные средства, реализующие один или несколько криптографических алгоритмов (шифрование, выработка и проверка электронной цифровой подписи, хэширование, имитозащита) и

криптографические протоколы, а также функции управления криптографическими ключами и функциональные возможности безопасности;

средства технической защиты информации – технические, программные, программно-аппаратные средства, предназначенные для защиты информации от несанкционированного доступа и несанкционированных воздействий на нее, блокирования правомерного доступа к ней, иных неправомерных воздействий на информацию, а также для контроля ее защищенности;

угроза – потенциально возможное событие, явление или процесс, которые посредством воздействия на компоненты информационной системы могут привести к нанесению ущерба;

целостность – свойство информации сохранять свое информационное содержание и однозначность интерпретации в условиях случайных или преднамеренных воздействий.

24. В Политике используются следующие обозначения и сокращения:

ИС – информационная система;

ЛПА – локальные правовые акты;

НПА – нормативные правовые акты;

ОАЦ – Оперативно-аналитический центр при Президенте Республики Беларусь;

ПО – программное обеспечение;

СЗИ – система защиты информации.

НОРМАТИВНЫЕ ССЫЛКИ

В Политике использованы ссылки на следующие нормативные правовые акты:

1. Закон Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации».

2. Приказ Оперативно-аналитического центра при Президенте Республики Беларусь 20 февраля 2020 г. № 66 «О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449».