УТВЕРЖДЕНО
Приказ главного врача
учреждения здравоохранения
«Гомельская городская
клиническая больница № 2»

_____ М.Н. Михасёв
«12» июля 2025 г.

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ
ИНФОРМАЦИОННОЙ СИСТЕМЫ
УЧРЕЖДЕНИЯ ЗДРАВООХРАНЕНИЯ
«ГОМЕЛЬСКАЯ ГОРОДСКАЯ КЛИНИЧЕСКАЯ БОЛЬНИЦА №2»

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

На 23 листах

Гомель, 2025

СОДЕРЖАНИЕ

1.

КОНТРОЛЬ ВЕРСИЙ ДОКУМЕНТА

Версия	Дата утверждения	Причина изменений
1.0	12.07.2025	Разработка документа

Порядок пересмотра документа

В целях постоянного совершенствования настоящей Политики информационной безопасности (далее – Политика) в соответствии с изменениями условий деятельности учреждения здравоохранения «Гомельская городская клиническая больница № 2» (далее – Учреждение), законодательства Республики Беларусь, требований национальных стандартов, которым должно соответствовать Учреждение, изменениями в организационной структуре или в информационной инфраструктуре Учреждения требуется регулярно пересматривать Политику – не реже одного раза в год. По результатам пересмотра в Политику в случае необходимости вносятся изменения.

Внеплановый пересмотр настоящей Политики может быть выполнен по результатам расследований инцидентов или в случае внесения существенных изменений в деятельность Учреждения.

1. Обозначения и сокращения

ИБ	информационная безопасность
ИС	информационная система
СЗИ	система защиты информации
СКЗИ	средства криптографической защиты информации
Учреждение	учреждение здравоохранения «Гомельская городская клиническая больница № 2»

2. Термины и определения

В настоящей политике информационной безопасности применяются термины и их обозначения, установленные в законодательных актах Республики Беларусь в области информации, информатизации и защиты информации:

Актив – средства вычислительной техники, телекоммуникационное оборудование, системное и прикладное программное обеспечение, информационные ресурсы, входящие в состав информационной системы.

Аутентификация – установление подлинности субъекта на основании проверки соответствия предъявленных им идентификатора и ключа аутентификации. Проверка принадлежности субъекту доступа предъявленного им идентификатора (подтверждение подлинности).

Доступ к информации – возможность получения информации и пользования ею.

Доступность – свойство информации быть доступной и используемой по запросу со стороны уполномоченного персонала.

Идентификация – процедура установления субъекта или объекта по предъявляемому им идентификационному признаку (например, пользователя по логину, файла по контрольной сумме).

Информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

Информационная безопасность – обеспечение конфиденциальности, целостности и доступности информационных активов организации.

Информационная сеть – совокупность информационных систем либо комплексов программно-технических средств информационной системы, взаимодействующих посредством сетей электросвязи.

Информационная система – совокупность банков данных, информационных технологий и комплекса (комплексов) программно-технических средств.

Информационный ресурс – организованная совокупность документированной информации, включающая базы данных, другие совокупности взаимосвязанной информации в информационных системах.

Конфиденциальность – свойство информации, заключающееся в недоступности информации или не раскрытии её содержания для неавторизованных лиц, процессов и логических объектов.

Криптографическая защита информации – деятельность, направленная на обеспечение конфиденциальности, контроля целостности и подлинности информации с использованием средств криптографической защиты информации.

Несанкционированное воздействие на информацию – изменение или уничтожение информации, осуществляемое с нарушением установленных прав или правил.

Несанкционированный доступ к информации – доступ к информации, осуществляемый с нарушением установленных прав или правил разграничения доступа.

Пользователь информационной системы, информационной сети – субъект информационных отношений, получивший доступ к автоматизированной системе, информационной системе, информационной сети и пользующийся ими.

Система защиты информации – совокупность мер по защите информации, реализованных в информационной системе.

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.

Техническая защита информации – деятельность, направленная на обеспечение конфиденциальности, целостности, доступности и сохранности информации техническими мерами без применения средств криптографической защиты информации.

Целостность – свойство информации, заключающееся в обеспечении точности и полноты информации.

3. Общие положения

3.1 Политика информационной безопасности Учреждения разработана в соответствии с приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 20.02.2020 № 66 «О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019г. № 449».

3.2 Политика ИБ СЗИ ИС является основополагающим документом Учреждения в области информационной безопасности и устанавливает документально закрепленные общие намерения по обеспечению конфиденциальности, целостности, сохранности, подлинности и доступности информации.

3.3 Требования Политики ИБ обязательны к исполнению всеми работниками Учреждения. Ознакомление работников с Политикой ИБ осуществляется под расписку по форме согласно Приложению к настоящей Политике ИБ.

3.4 Настоящая Политика определяет цели и задачи Учреждения в области обеспечения информационной безопасности, обеспечивает надлежащий уровень информационной безопасности и является основой для всех подчиненных процессов, процедур, правил и документов по информационной безопасности в Компании.

3.5 Технические принципы и детализированные требования по реализации настоящей Политики определены в документе «Стандарт информационной безопасности».

3.6 Положения Политики ИБ должны быть учтены при заключении договоров (Соглашений о конфиденциальности) с организациями, взаимодействующими с Учреждением в качестве поставщиков и потребителей (пользователей) его информации, а также с разработчиками информационных систем, подрядных организаций, осуществляющих техническое обслуживание аппаратных средств и сопровождение программного обеспечения автоматизированных информационных систем Учреждения.

4. Общие сведения об информационной системе

4.1 Настоящая Политика применяется в системе защиты информации информационной системы Учреждения.

4.2 В ИС Учреждения обрабатывается и хранится информация, которая в соответствии с Законом Республики Беларусь «Об информации, информатизации и защите информации» от 10.11.2008 № 455-З и Законом Республики Беларусь от 07.05.2021 № 99-З «О защите персональных данных» отнесена к следующим категориям информации:

- информация о частной жизни физического лица;

- персональные данные;
- специальные персональные данные, за исключением биометрических и генетических персональных данных.

4.3 В соответствии с «Классами типовых информационных систем» (Приложение 1 к «Положению о порядке технической и криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено») ИС Учреждения отнесена к классу 3-ин, 3-спец.

4.4 Основные ресурсы Учреждения размещены на площадях Учреждения.

4.5 Доступ в сеть Интернет ИС Учреждения осуществляется уполномоченным поставщиком интернет-услуг РУП «Белтелеком» при котором реализованы следующие меры защиты информации (в соответствии с Приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 2 августа 2010 г. № 60 «Об утверждении положения о порядке определения уполномоченных поставщиков интернет-услуг»):

- обработка DNS-запросов пользователей с исключением прямого использования иностранных DNS-серверов;
- фильтрация трафика от вредоносного программного обеспечения и вторжений;
- защита от распределенных атак, направленных на нарушение доступности оказываемых услуг.

4.6 Функционирование официального сайта и электронной почты Учреждения осуществляется в рамках услуг уполномоченного провайдера хостинга ООО «Белорусские облачные технологии», в рамках которых реализованы следующие меры защиты информации:

- осуществляется полное резервное копирование информации официального сайта не реже одного раза в неделю;
- система обмена электронной почтой обеспечивает возможность блокирования незапрашиваемой информации (спама) и антивирусную защиту передаваемых сообщений;
- обеспечение защиты от атак на веб-приложения с использованием технологии инспекции SSL/TLS соединений;
- обеспечение функционирования системы аудита и протоколирования событий безопасности официального сайта со сроком хранения данной информации не менее одного года.

5. Цели создания системы защиты информации

5.1 Под СЗИ понимается такое состояние активов ИС при котором обеспечивается необходимый уровень конфиденциальности, целостности, подлинности, доступности и сохранности принимаемой, обрабатываемой, хранимой, отображаемой и передаваемой информации, а также защищенность самой ИС, бизнес-процессов и каналов информационного обмена, ресурсов и средств вычислительной техники, программного обеспечения, документации от несанкционированного доступа к ним.

5.2 Основными целями создания СЗИ активов ИС является:

- вовлечение высшего руководства Учреждения в управление процессами информационной безопасности;
- сохранение и неразглашение персональных данных, врачебной тайны, содержащихся в информационных системах (ресурсах);
- недопущение неправомерного доступа, уничтожения, модификации (изменения), копирования, распространения и (или) предоставления информации, блокирования правомерного доступа к персональным данным, врачебной тайне, содержащихся в информационных системах (ресурсах), а также иных неправомерных действий;
- минимизация ущерба от реализации угроз ИБ в отношении информационных систем (ресурсов);
- осуществление контроля за соблюдением требований ИБ и порядком использования активов ИС, установленных в документации и локальных актах;
- повышение осведомленности работников Учреждения в области ИБ.

5.3 Меры ИБ, реализуемые в отношении активов ИС, должны обеспечивать непрерывность осуществления деятельности Учреждения по назначению.

5.4 Для достижения основных целей СЗИ активов ИС должна обеспечивать решение следующих задач:

- своевременное выявление и прогнозирование источников угроз активам ИС;
- оценка возможного воздействия угроз на активы ИС и потенциальных последствий такого воздействия;
- оперативное реагирование на угрозы безопасности информации путем принятия своевременных мер по недопущению нарушения ИБ активов ИС и (или) снижению негативных последствий нарушения безопасности;
- назначение работникам Учреждения, а также сотрудникам сторонних организаций прав доступа и полномочий по доступу к активам ИС только в том объеме, который необходим им для выполнения своих служебных обязанностей или работ, предусмотренных условиями договоров;

- предоставление доступа к активам ИС только авторизованным пользователям после их успешной идентификации и аутентификации, предотвращение и блокирование попыток неавторизованного доступа к активам ИС;
- ограничение физического доступа посторонних лиц к средствам обработки и хранения информации;
- защита персональных данных и врачебной тайны от раскрытия при их передаче по общедоступным каналам электросвязи между удаленными пользователями и узлами обработки информации;
- контроль обеспечения ИБ активов ИС при использовании услуг по разработке, модернизации, внедрению, обслуживанию, сопровождению, резервированию и администрированию ИС или их компонентов, оказываемых сторонними организациями;
- заблаговременное принятие эффективных мер по восстановлению безопасного состояния активов ИС на случай возможного нарушения ИБ в результате реализации угроз;
- надлежащее применение криптографических средств защиты информации в соответствии с законодательством;
- контроль состояния защищенности и эффективное управление ИБ активов ИС.

6. Основные угрозы информационной безопасности

6.1 Согласно положениям данной Политики, Учреждение осуществляет защиту информации, распространение и (или) предоставление которой ограничено, путем:

- проведения комплекса правовых, организационных и технических мер по обеспечению целостности, конфиденциальности и доступности информации;
- выявления потенциальных угроз и уязвимостей информационной безопасности, анализа и оценки рисков информационной безопасности, исключения либо минимизации выявленных рисков, предотвращения инцидентов информационной безопасности.

6.2 Основными источниками угроз для ИС являются:

- ошибки работников, как результат недостатка знаний, неисполнения установленных требований, процедур и недостаточность документированных требований в области информационной безопасности;
- негативные факторы технического и социального характера (вирусная активность, хакерская активность, мошенничество, превышение полномочий, криминальная деятельность и т.п.);

- негативные факторы природного и техногенного характера.

6.3 Основными угрозами безопасности информации общего характера являются:

- утечки информации;
- неавторизованный доступ;
- вредоносные программы;
- атаки хакеров;
- отказ в обслуживании (DDoS-атаки);
- таргетированные атаки;
- спам;
- фишинг;
- шпионское программное обеспечение;
- сбои и отказы инженерной инфраструктуры.

6.4 В отношении типовых телекоммуникационных и информационных систем актуальны следующие основные типы угроз безопасности информации:

- угрозы создания нештатных режимов работы;
- угрозы доступа (проникновения) в операционную (системную) среду;
- угрозы несанкционированного удаленного доступа к оборудованию и системам;
- подмена доверенного объекта сети;
- навязывание ложного маршрута;
- внедрение ложного объекта сети;
- угрозы программно-математического воздействия.

6.5 Реализация угрозы приводит к нанесению ущерба для Учреждения (финансовые потери; нарушение деловой репутации; негативная реакция клиентов, регулирующих органов и т.д.). Снижение вероятности нанесения ущерба (снижение риска) напрямую связано с выявлением и устранением уязвимостей защищаемых активов Учреждения.

7. Основные принципы обеспечения защиты информации

С целью установления индивидуальной ответственности и минимизации рисков утечки информации, следует соблюдать следующие принципы и методы:

7.1 Идентификация – это метод, позволяющий однозначно различать людей или системы. Каждый человек должен быть идентифицирован путем проверки его личности, до того, как ему будет предоставлен доступ к защищаемой информации. Каждый актив ИС должен быть идентифицированы до того, как его подключат к ИС. Действия каждого человека в системе, сервисе должны быть однозначно идентифицированы.

7.2 Авторизация – предоставление определённому лицу или группе лиц прав на выполнение определённых действий, а также процесс проверки (подтверждения) данных прав при попытке выполнения этих действий.

7.3 Аутентификация – подтверждение подлинности пользователей. Осуществляется путем проверки наличия у пользователей каких-либо специальных устройств (бесконтактных электронных и механических ключей и т.д.), путем проверки пароля, путем проверки иных уникальных характеристик.

7.4 Ответственность – индивидуальная ответственность за предоставление, изъятие доступа к информации, получение доступа к информации, обращение с информацией в соответствии с установленными правилами.

7.5 Деловая необходимость – защищаемая информация может быть доступна, сохранена, прочитана, изменена или передана только если в этом есть потребность для деятельности Учреждения. Права доступа к защищаемой информации должны изыматься, как только потребность в таком доступе отсутствует.

7.6 Наименьшие привилегии – учетные записи должны быть ограничены минимальным уровнем прав доступа для удовлетворения деловой необходимости.

7.7 Разделение обязанностей – концепция, при которой для выполнения задачи требуется более одного человека с целью предотвращения мошенничества и ошибок.

7.8 Обязанности по ИБ – соблюдение правил, политик, стандартов и процедур по информационной безопасности.

7.9 Журналы событий – файлы или базы данных, регистрирующие и хранящие действия пользователей, события информационной безопасности, используемые для мониторинга безопасности и расследования инцидентов.

8. Основные положения обеспечения защиты информации

8.1 В рамках деятельности по защите информации в Учреждении реализуются сбалансированные взаимодополняющие правовые, организационные и технические меры.

8.2 К основным правовым мерам, направленным на защиту информации в ИС, относятся:

- соблюдение законодательства Республики Беларусь в области защиты информации;
- разработка и распределение в установленном порядке должностных обязанностей работников, отвечающих за ИБ;

- внесение изменений и дополнений в организационно-распорядительные документы (положения о структурных подразделениях, должностные инструкции, инструкции пользователей, трудовые договоры и тому подобные) по вопросам обеспечения ИБ;
- подготовка приказов, распоряжений, методических материалов, касающихся вопросов защиты информации;
- подготовка документов по вопросам регламентации отношений между Учреждением и сторонними организациями, предоставляющими услуги, в части обеспечения безопасности активов ИС и правил разрешения проблемных ситуаций, связанных с нарушением требований ИБ со стороны поставщиков услуг;
- согласование договоров или соглашений, в которых устанавливаются условия пользования информацией, а также ответственность сторон по договору за нарушение указанных условий.

8.3 Организационные меры регламентируют процессы функционирования ИС, использование ее ресурсов, деятельность персонала, а также порядок взаимодействия пользователей с ИС таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз ИБ, или снизить размер потерь в случае их реализации.

8.4 К основным организационным мерам относятся:

- проведение учета и категорирования активов ИС с назначением владельцев активов ИС, поддержание учетных данных в актуальном состоянии;
- выявление наиболее вероятных потенциальных угроз для активов ИС, выявление уязвимых мест процессов обработки, передачи и хранения информации в обеспечении ИБ активов ИС;
- определение порядка назначения, изменения, утверждения и предоставления работникам Учреждения и сторонних организаций необходимых полномочий по доступу к активам ИС;
- разработка правил управления доступом к активам ИС, режимов обработки данных и доступа к ним;
- определение перечня необходимых мер по обеспечению штатного функционирования ИС и ее компонентов в критических ситуациях, возникающих в результате несанкционированного доступа к активам ИС, сбоев и отказов технических средств, ошибок программного обеспечения и пользователей, стихийных бедствий;
- определение порядка и правил резервного копирования и восстановления информации;
- определение порядка и правил антивирусной защиты активов ИС;

- определение порядка доступа работников Учреждения к внешним сетям, в том числе к глобальной компьютерной сети Интернет, а также правил надлежащего использования общедоступных сервисов;
- определение порядка учета, выдачи, использования и хранения внешних носителей информации, используемых для создания и хранения резервных и архивных копий информации, а также для информационного обмена между компонентами ИС или работниками;
- установление правил обеспечения безопасности при использовании работниками мобильных средств обработки и хранения данных, удаленном доступе к активам ИС с использованием таких средств.
- организация контроля доступа в помещения, в которых размещено серверное и коммуникационное оборудование ИС;
- организация учета, хранения, использования и уничтожения документов и носителей с информацией ограниченного распространения;
- контроль за соблюдением работниками Учреждения и сторонних организаций, оказывающих услуги или пользующихся информационными услугами Учреждения, требований и правил по обеспечению ИБ активов ИС, установленных настоящей Политикой ИБ и локальными правовыми актами;
- контроль за формированием и реализацией требований ИБ при разработке и модернизации программного и аппаратного обеспечения ИС или ее отдельных компонентов;
- периодический анализ состояния и оценка эффективности применяемых мер по защите информации;
- определение и реализация мер сетевой безопасности активов ИС;
- поддержание в актуальном состоянии проектной и эксплуатационной документации на ИС и ее компоненты с отражением в ней аспектов, связанных с обеспечением ИБ;
- инструктаж, обучение и информирование работников Учреждения, а также работников сторонних организаций по выполнению требований ИБ при работе с активам ИС;
- определение категорий лиц, имеющих доступ в помещения, в которых установлены технические средства обработки и защиты информации ИС;
- разграничение доступа к информации по кругу лиц и характеру информации.

8.5 К основным техническим мерам по защите информации в ИС относятся:

- настройка доступа в ИС только авторизованных пользователей после прохождения успешной идентификации и аутентификации;
- выполнение резервного копирования данных и информации;

- применение сертифицированных средств защиты и лицензионного программного обеспечения;
- применение СКЗИ информации для защиты конфиденциальности, целостности и подлинности информации при ее передаче по каналам связи общего доступа;
- контроль функционирования и управление применяемыми в ИС средствами защиты информации;
- регистрация событий безопасности, связанных с действиями пользователей при работе с активами ИС и управлением режимами функционирования компонентов ИС и средств защиты информации;
- анализ журналов аудита, своевременное обнаружение нарушений ИБ и принятие соответствующих мер по восстановлению безопасного состояния;
- ликвидация или снижение последствий нарушения ИБ (локализация);
- применение следующих мер обеспечения защиты активов ИС от угроз при взаимодействии с глобальной компьютерной сетью Интернет и сторонними информационными системами:
  - фильтрация сетевых пакетов в соответствии с задаваемыми правилами на основе IP-адресов отправителя и получателя, разрешенных портов, протоколов и приложений;
  - управление сетевым доступом к сегментам ИС;
  - перенаправление сетевых адресов для сокрытия топологии сети;
  - обнаружение атак с использованием известных шаблонов атак;
  - защита от атак типа «отказ в обслуживании»;
  - обновление базы сигнатур подсистемы обнаружения вторжений;
  - антивирусная фильтрация трафика, получаемого из Интернета и антивирусная защита активов ИС;
- регистрация событий ИБ с заданным уровнем детализации;
- обеспечение отказоустойчивости аппаратных средств защиты информации;
- размещение серверов, предоставляющих общедоступные (доступные из Интернета) сервисы, и серверов, имеющих прямой доступ в Интернет, в выделенном (изолированном от ИС) сегменте сети – демилитаризованной зоне.

9. Порядок применения средств защиты информации

9.1 При осуществлении технической и криптографической защиты информации, обрабатываемой в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, должны использоваться средства технической и криптографической защиты информации, имеющие сертификат соответствия Национальной

системы подтверждения соответствия Республики Беларусь или положительное экспертное заключение по результатам государственной экспертизы, проводимой Оперативно-аналитическим центром при Президенте Республики Беларусь.

9.2 Параметры и характеристики применяемых средств защиты информации должны реализовывать технические меры по обеспечению информационной безопасности, необходимые для конкретных информационных систем.

9.3 Применяемые средства защиты информации должны быть обеспечены гарантийной и технической поддержкой со стороны изготовителей (разработчиков) этих средств или их представителей.

9.4 В ходе внедрения средств технической и криптографической защиты информации осуществляются их монтаж и наладка в соответствии с документацией на систему защиты информации, рекомендациями изготовителя, требованиями по совместимости средств криптографической защиты информации и ограничениями, указанными в сертификате соответствия.

10. Обязанности субъектов учреждения

10.1 Субъектами информационных отношений Учреждения являются:

- Министерство здравоохранения, в качестве собственника информации распространение и (или) предоставление которой ограничено, но не относящейся к государственным секретам;
- Учреждение, как владелец (оператор) информационных систем (ресурсов) и их компонентов;
- пользователи ИС Учреждения;
- юридические лица, в качестве информационных посредников и при необходимости операторов информационных систем;
- государственные органы и организации, юридические лица, в качестве пользователей информации и информационных систем (ресурсов).

10.2 Ответственные и должностные лица субъектов информационных отношений:

- руководство Учреждения, в соответствии с возложенными на них функциями;
- работники отдела автоматизированной системы управления и назначенные администраторы безопасности или получившие доступ к СЗИ в рамках выполнения своих функциональных обязанностей;
- администраторы, осуществляющие обеспечение безопасного функционирования информационных систем (ресурсов), их компонентов и инфраструктуры (далее – администратор системы);

- должностные лица поставщиков услуг и юридических лиц, осуществляющие гарантийное или сервисное обслуживание информационных систем (ресурсов) и их компонентов;

- должностные лица государственных органов и организаций, юридических лиц, в том числе представители организаций, которые получили доступ к информационным системам (ресурсам) и/или услугам Учреждения (далее – пользователи).

10.3 Общее руководство обеспечением ИБ осуществляет главный врач Учреждения.

10.4 Руководители структурных подразделений Учреждения принимают меры по обеспечению сохранности информации, распространение и (или) предоставление которой ограничено, в подотчетных подразделениях и в пределах своей компетенции осуществляют контроль за соблюдением подчиненными работниками требований настоящей Политики ИБ и локальных правовых актов по ИБ Учреждения.

10.5 Должностные лица поставщиков услуг и юридических лиц имеют обязательства в рамках договорных отношений.

10.6 Должностные лица государственных органов наделяются полномочиями в соответствии с законодательством Республики Беларусь.

10.7 Работники отдела автоматизированной системы управления осуществляют организацию, планирование, сопровождение, координацию и контроль работ по обеспечению ИБ в Учреждении, а также выполняют следующие функции:

- обеспечение соблюдения требований законодательства в области ИБ;
- разработка, внедрение, обеспечение функционирования и развитие СЗИ активов ИС;
- определение требований по защите информации в процессе разработки, внедрения, обеспечения функционирования и развития активов ИС;
- техническую и криптографическую защиту обрабатываемой в Активах информации, распространение и (или) предоставление которой ограничено, не содержащей сведения, отнесенные к государственным секретам;
- защиту активов ИС в соответствии с мерами по ИБ, установленными для данных активов ИС;
- прогнозирование, предупреждение и выявление инцидентов ИБ, реагирование на них;
- пресечение действий нарушителей ИБ;
- регистрация нарушений ИБ, анализ и обобщение информации о них, ведение базы инцидентов ИБ, разработка процедур реагирования на инциденты;

- разработка, внедрение и поддержание в актуальном состоянии настоящей Политики ИБ и организационно-распорядительной документации, регламентирующей вопросы обеспечения ИБ в Учреждении;
- учет и категорирование активов ИС;
- контроль соблюдения работниками Учреждения и сторонних организаций требований по защите информации, установленных настоящей Политикой ИБ и локальными правовыми актами, анализ и обобщение результатов контроля;
- взаимодействие с работниками по вопросам обеспечения ИБ (информирование, обучение, консультирование, повышение осведомленности);
- информирование главного врача, его заместителей, руководителей структурных подразделений Учреждения (владельцев Актива) об угрозах и инцидентах ИБ, влияющих на деятельность Учреждения;
- взаимодействие с регулирующими органами и поставщиками телекоммуникационных услуг по вопросам, связанным с ИБ.

10.8 Для управления доступом к информационной системе приказом главного врача Учреждения назначается ответственный за техническую и криптографическую защиту информации.

10.9 Ответственному за техническую и криптографическую защиту информации предоставляются права доступа к информационной системе, в объеме, необходимом и достаточном для выполнения возложенных на него обязанностей.

10.10 С учетом специфики информационной системы, обязанности ответственного за техническую и криптографическую защиту информации могут быть расширены в установленном порядке.

10.11 Ответственный за техническую и криптографическую защиту информации поддерживает безопасное состояние ИС и осуществляет:

- назначение (изменение) или блокирование при обнаружении нарушений прав доступа пользователя к информационной системе (ресурсу);
- предоставление доступа к информационной системе (ресурсу);
- контроль состояния информационной системы (ресурса) по ключевым показателям в процессе эксплуатации;
- анализ событий безопасности с целью выявления нарушений безопасности информационной системы (ресурса) или попыток несанкционированных действий;
- контроль и своевременное блокирование действий пользователей, которые могут нарушить нормальное функционирование информационной системы (ресурса);

- создание резервных копий информационной системы (ресурса) и архивных файлов;
- восстановление безопасного состояния информационной системы (ресурса) в случае его нарушения;
- администрирование активов СЗИ;
- контроль работы всех пользователей и администраторов системы по вопросам соблюдения требований ИБ;
- обеспечение функционирования и модернизации серверного, коммуникационного оборудования и вычислительной техники;
- подготовку предложений по развитию и модернизации СЗИ;
- информирование вышестоящего руководителя обо всех инцидентах, связанных с нарушением ИБ, выявленных в ИС.

10.12 Пользователи ИС обязаны:

- соблюдать установленные требования и правила ИБ;
- содействовать выявлению и предотвращению реализации угроз ИБ;
- содействовать предупреждению и выявлению инцидентов ИБ, а также минимизации их последствий их негативного воздействия на активы ИС (локализации);
- незамедлительно информировать вышестоящего руководителя и руководителя структурного подразделения (владельца актива) о предполагаемых угрозах и возможных инцидентах ИБ.

11. Инциденты информационной безопасности

11.1 Все факты нарушения информационной безопасности могут быть обнаружены как работниками Учреждения, так и автоматическими средствами (системами анализа журналов аудита, межсетевыми экранами, системами обнаружения вторжений, антивирусным программным обеспечением и т.п.).

11.2 В Учреждении должен быть установлен порядок информирования, мониторинга и регистрации инцидентов.

11.3 По каждому инциденту, связанному с нарушением информационной безопасности в Учреждении, проводится расследование. Ответственность за проведение расследования инцидента возлагается на руководителя подразделения, в котором произошел инцидент, а также на ответственного за техническую и криптографическую защиту информации. Результаты расследования включаются в журнал инцидентов.

11.4 По уровню критичности инциденты информационной безопасности делятся на следующие уровни:

- низкий;
- высокий.

11.5 По инцидентам высокого уровня должно происходить информирование руководства Учреждения и Национального центра обеспечения кибербезопасности.

12. Физическая безопасность

12.1 Для минимизации риска несанкционированного доступа к активам ИС, а также нарушения их конфиденциальности, целостности и доступности должны применяться методы контроля физического доступа и защиты от воздействия окружающей среды.

12.2 Доступ в служебные помещения (серверные и иные помещения) должен предоставляться конкретным работникам, что позволяет провести его идентификацию. Физический доступ предоставляется в соответствии с принципами деловой необходимости и только в том объеме, который необходим для выполнения соответствующих задач.

12.3 Основные активы ИС должны быть обеспечены системой бесперебойного питания, средствами пожаротушения и кондиционирования.

13. Порядок взаимодействия с иными информационными системами и сетями

13.1 Взаимодействие с иными информационными системами и сетями должно осуществляться на договорной основе и способами, не снижающими уровень защиты информации.

13.2 При составлении договоров, предусматривающих доступ сторонних организаций (информационных систем) к ИС, необходимо учитывать следующие вопросы:

- обязательства о конфиденциальности;
- разрешенные способы доступа, а также использование и контроль за использованием уникальных идентификаторов пользователей и паролей;
- наименование каждого предоставляемого информационного ресурса;
- право отслеживать действия пользователей;
- ограничение на копирование информации;
- применение сертифицированных средства канального (линейного) шифрования;
- меры по обеспечению защиты от компьютерных вирусов.

13.3 Взаимодействие с информационными системами других организаций осуществляется в целях обмена информацией, необходимой для реализации функций, возложенных на Учреждение.

14. Контроль и ответственность

14.1 Ответственность за исполнение положений настоящей Политики ИБ возлагается на главного врача Учреждения.

14.2 Ответственность за контроль исполнения положений настоящей Политики ИБ возлагается на начальника отдела автоматизированной системы управления Учреждения.

14.3 Руководители структурных подразделений Учреждения, обеспечивают ознакомление своих подчиненных работников с Политикой ИБ под роспись.

14.4 Пользователи ИС Учреждения несут персональную ответственность за несоблюдение требований настоящей Политики.

14.5 Неисполнение или некачественное исполнение работниками Учреждения требований Политики ИБ может повлечь лишение доступа к ИС или ее компонентам, а также применение к виновным лицам правовых мер воздействия, степень которых определяется установленным в Учреждения порядком и требованиями законодательства Республики Беларусь.

Приложение
к Политике информационной
безопасности Учреждения
ФОРМА

Лист ознакомления
с Политикой информационной безопасности Учреждения

_____

(наименование подразделения)

№ п/п	Фамилия И.О.	Дата ознакомления	Подпись