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»

СТАНДАРТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
На 29 листах

Гомель, 2025

КОНТРОЛЬ ВЕРСИЙ ДОКУМЕНТА

Версия	Дата утверждения	Причина изменений
1.0	12.07.2025	Разработка документа

Порядок пересмотра документа

В целях постоянного совершенствования настоящего Стандарта информационной безопасности (далее – Стандарт) в соответствии с изменениями условий деятельности учреждения здравоохранения «Гомельская городская клиническая больница № 2» (далее – Учреждение), законодательства Республики Беларусь в области защиты информации, политики информационной безопасности Учреждения, требований национальных и международных стандартов, которым должна соответствовать Учреждение, изменениями в организационной структуре или в информационной инфраструктуре Учреждения требуется регулярно пересматривать Стандарт – не реже одного раза в год. По результатам пересмотра в Стандарт в случае необходимости вносятся изменения.

Внеплановый пересмотр настоящего Стандарта может быть выполнен по результатам расследований инцидентов или в случае внесения существенных изменений в бизнес-процессы Учреждения.

СОДЕРЖАНИЕ

1. Общие положения

1.1. В Стандарте определены минимальные технические детализированные требования по соблюдению, внедрению Политики информационной безопасности.

1.2. В настоящем Стандарте определены минимальные технические требования безопасной конфигурации, настройки, организации сервисов, систем и сети Учреждения.

2. Назначение и область применения

2.1. Настоящий Стандарт разработан с целью выполнения требований законодательства Республики Беларусь в области защиты информации и представляет собой набор технических детализированных требований по внедрению и соблюдению Политики информационной безопасности Учреждения.

2.2. Настоящий Стандарт распространяется:

- на все бизнес-процессы Учреждения;
- на всю информацию, за которую несет ответственность Учреждение, и которая представлена в разных формах: бумажной, электронной, устной;
- на все активы ИС Учреждения, которые хранят, передают и обрабатывают информацию, за которую несет ответственность Учреждение.

2.3. Настоящий Стандарт обязателен для исполнения всеми работниками, а также лицами, работающими с информацией, принадлежащей Учреждению, в рамках, установленных договорными обязательствами.

3. Сетевая инфраструктура

3.1. Основные требования к сетевой инфраструктуре

3.2. Все сетевые устройства, подключаемые к сети Учреждения должны быть индивидуально идентифицируемы (серийный номер, инвентарный номер, MAC и т.д.) в принятых в Учреждении системах учета.

3.3. За действия в отношении сетевых устройств отвечают работники, ответственные за их эксплуатацию.

3.4. Доступ сетевых устройств подрядчиков и партнеров к внутренней сети Учреждения разрешен только после заключения соответствующего договора и соглашения о неразглашении информации.

3.5. Должно быть обеспечено сегментирование (изоляция) сети управления активами информационной системы, средствами защиты информации от сети передачи данных.

3.6. Публикация сетевых сервисов, протоколов, портов управления (например, SSH, RDP, HTTPS и т.д.) в сеть Интернет с целью удаленного администрирования, управления сервисами, системами запрещено.

3.7. Не допускается использование небезопасных уязвимых сетевых сервисов (HTTP, FTP, SNMPv1 и т.д.) как внутри сети, так и при коммуникации с недоверенными сетями, для публикации в сеть Интернет. При этом должно обеспечиваться использование стойких к кибератакам сетевых сервисов и протоколов (например, HTTPS, SFTP, SNMPv3 и т.д.) для обеспечения защиты передаваемой информации, недопущения эксплуатации общеизвестных уязвимостей.

3.8. Должен быть обеспечен централизованный сбор и хранение сведений о DNS-запросах активов информационной системы, средств защиты информации в течение установленного срока хранения, но не менее одного месяца.

3.9. **Межсетевые экраны, маршрутизаторы, защита от вторжений**

3.10. Любое взаимодействие с внешними ИС должно осуществляться через межсетевой экран.

3.11. На всех межсетевых экранах должны быть определены глобальные запрещающие правила, ограничивающие любые соединения, кроме явно разрешенных. Это является базовой конфигурацией при вводе межсетевого экрана в эксплуатацию. Сброс настроек межсетевых экранов должен восстановить базовую конфигурацию, запрещающую любые соединения, кроме явно разрешенных.

3.12. Входящие и исходящие разрешающие правила межсетевого экранирования между зонами безопасности должны быть ограничены по IP-адресам, портам и протоколам. Все внедряемые правила межсетевого экранирования должны быть задокументированы в виде запроса с обоснованием бизнес-необходимости, согласованы непосредственным руководителем инициатора и подтверждены ответственным за информационную безопасность. Запрещается внедрение, изменение правил межсетевого экранирования без специализированного согласованного запроса согласно требованиям данного пункта.

3.13. Каждое изменение в правилах межсетевых экранов и маршрутизаторов должно быть отслеживаемо, протоколируемо и иметь возможность проверки.

3.14. Все правила межсетевого экранирования, требуемые для обеспечения бизнес-процессов, должны иметь возможность восстановления из резервных копий конфигураций.

3.15. Запрашиваемые правила межсетевого экранирования должны быть ограничены во времени, максимум 1 год.

3.16. Сетевой трафик (входящий и исходящий) между сетью Учреждения и недоверенными сетями (Интернет, сети внешних организаций и т.д.) должен проверяться системой обнаружения и предотвращения сетевых атак.

4. Резервное копирование информации

4.1. Должен быть назначен работник, ответственный за резервное копирования информации основных активов ИС.

4.2. В Учреждении должен быть утвержден перечень активов ИС, подлежащих резервному копированию. Для каждого актива должна быть определена частота создания резервной копии.

4.3. Для каждого актива ИС, подлежащего резервному копированию, должен быть установлен максимальный срок хранения резервной копии. Срок хранения резервной копии определяется с учетом бизнес-необходимости Учреждения.

4.4. Срок хранения резервной копии для каждого актива ИС определяется владельцем соответствующего актива.

4.5. Перечень активов ИС, подлежащих резервному копированию, частота резервного копирования каждого актива и сроки хранения резервной копии для каждого актива включаются в План резервного копирования.

4.6. Должно быть обеспечено резервное копирование конфигурационных файлов телекоммуникационного оборудования.

4.7. Резервное копирование информации, а также проверка успешности, выполняются по расписанию ответственным за резервное копирование на основе Плана резервного копирования с помощью программных средств резервного копирования.

4.8. По итогам выполнения процедуры резервного копирования в протоколах событий системы резервного копирования фиксируются:

- дата и время проведения резервного копирования;
- информационная система (ресурс), содержащая тот или иной актив, которая была зарезервирована;
- результат выполнения задачи;
- иные комментарии при необходимости.

4.9. Восстановление информации из резервной копии производится по запросу от владельца актива ИС на основании зарегистрированного запроса (электронного письма) на восстановление данных.

4.10. Должно регулярно производится тестирование процедуры восстановления для важных активов ИС.

5. Безопасность учетных записей

5.1. Рабочие учетные записи используются работниками Учреждения и представителями внешних организаций при необходимости удаленного доступа к сети Учреждения.

5.2. В Учреждении определены следующие типы рабочих учетных записей:

Типы корпоративных учетных записей	Описание
Персонифицированные: - для работников Учреждения; - для представителей внешних организаций (партнеры, контрагенты).	Учетные записи пользователей и администраторов, которые используются для доступов к сервисам, системам для выполнения должностных обязанностей и поддержки, администрирования.
Сервисные	Учетные записи, которые используются для автоматизированных действий, интеграций сервисов, систем и которые не предназначены для использования с целью поддержки и администрирования (как правило сервисные учетные записи содержат в наименовании сокращенное имя технического сервиса, а в описании назначение учетной записи).
Стандартные учетные записи (встроенные)	Учетные записи, предусмотренные производителями и которые появляются в системе автоматически после ее инсталляции.

5.3. Любой доступ к активам ИС осуществляется с использованием реквизитов доступа – учетной записи и пароля, или других механизмов аутентификации.

5.4. За реквизиты доступа - учетная запись/пароль ответственность несет только одно лицо. Одно лицо может иметь несколько учетных записей.

5.5. Запрещено коллективно использовать персонифицированные учетные записи, а также регистрироваться и работать в системе под чужой учетной записью.

5.6. Все действия, совершенные под учетной записью, расцениваются как действия работника Учреждения либо представителя внешней организации, которому принадлежит учетная запись.

5.7. Использование сервисных учетных записей для осуществления пользовательских или административных действий запрещено.

5.8. Реквизиты доступа к учетной записи должны храниться в тайне. Хранить и передавать реквизиты доступа в открытом виде запрещено. Для паролей должно использоваться хэширование при хранении, шифрование при передаче.

5.9. Использование встроенных учетных записей для осуществления пользовательских или административных действий также запрещается, вместе с тем допускается их использование лишь в исключительных случаях, как правило при возникновении чрезвычайной необходимости.

5.10. Для встроенных УЗ должны быть назначены пароли, отличные от установленных производителем. К ним предъявляются требования, аналогичные требованиям к паролям сервисных УЗ.

5.11. Рекомендуется, по возможности, заблокировать встроенные, стандартные учетные записи. В случае невозможности блокировки обязательно должен быть сменен и установлен пароль согласно требованиям данного Стандарта.

5.12. Владельцем персонифицированной учетной записи является работник, которому она выдана для исполнения должностных обязанностей.

5.13. Владельцем сервисной учетной записи является работник, который ее заказал.

5.14. Владельцами встроенных, стандартных учетных записей являются владельцы активов ИС, на которых данные учетные записи существуют.

5.15. Запрещено использовать рабочие реквизиты доступа на сторонних Интернет-ресурсах и приложениях.

5.16. Каждая рабочая учетная запись как минимум должна иметь парольную защиту. В случае использования другого механизма аутентификации, такой механизм аутентификации должен предотвращать возможность несанкционированного доступа без знания факторов аутентификации и без прохождения процесса аутентификации со стороны владельца учетной записи.

5.17. В случае технических ограничений по использование центрального механизма аутентификации допускается использование встроенных механизмов аутентификации, но в обязательном порядке такие механизмы должны быть настроены согласно требованиям настоящего раздела.

5.18. Ко всем механизмам аутентификации, использующим пароли, предъявляются следующие требования:

- механизм аутентификации должен требовать периодическое изменение пароля;
- механизм аутентификации должен запрещать использование паролей, недостаточно стойких к подбору;
- механизм аутентификации должен обеспечивать стойкую длину и сложность паролей;
- механизм аутентификации должен проверять подлинность пользователя при смене пароля;

- механизм аутентификации должен запрещать использование повторных паролей.

5.19. При заведении учетной записи администратором устанавливается первоначальный пароль, который генерируется случайным образом согласно требованиям парольных политик. При первом сеансе аутентификации первоначальный пароль должен быть изменен владельцем учетной записи.

5.20. Пароль должен отвечать требованиям безопасности:

- минимальная длина пароля для пользователей ИС - 8 знаков. Крайне рекомендуется использовать длинные парольные фразы (от 13 символов), лёгкие для запоминания;
- пароль не должен основываться на каком-либо одном слове, выданном идентификаторе, имени, логине, кличке, паспортных данных, e-mail, URL сайта или именем домена, названием приложения или Учреждения и т.д. (например, "Ivanov" не может иметь пароли "123van", "vano27xyz" и др.);
- пароли не должны основываться на типовых шаблонах и идущих подряд на клавиатуре или в алфавите символов, например, таких, как: qwerty, 1234567, abcdefgh и т.д.

5.21. Пароль необходимо регулярно менять каждые пол года.

5.22. Новый пароль должен отличаться от предыдущего пароля не менее чем на 3 символа.

5.23. Пароли должны содержать:

- строчные латинские буквы: abcd...xyz;
- прописные латинские буквы: ABCD...XYZ;
- цифры: 123...90;
- минимальное количество заглавных и прописных букв, цифр - по 1 символу.

В паролях рекомендуется использовать специальные символы (: ! @ # $ % ^ & * ( ) - _ += ; : , ./ ? \ | ` ~ [ ] { }), пробел и знаки препинания (если возможно в соответствии с настройками активов ИС).

5.24. Для сервисных учетных записей дополнительно к указанным в п.6.22 настоящего Стандарта применяются следующие правила:

- минимальная длина пароля - 30 знаков,
- минимальное количество заглавных и прописных букв, цифр и специальных символов - по 5 символов.

5.25. Если в эксплуатационной документации к ИС предъявляются более жесткие требования по парольной защите, администратор активов ИС, ответственный за сопровождение эксплуатации ИС, руководствуется эксплуатационной документацией и настраивает ИС с более жесткими требованиями по парольной защите.

5.26. В ИС не должно быть ограничений на максимальную длину пароля / увеличить допустимый максимум длины пароля до 64 символов (если возможна реализация в ИС).

5.27. В ИС должна быть обеспечена возможность использовать все печатные символы ASCII, пробелы и символы UNICODE (если возможна реализация в ИС).

5.28. Пароли должны проверяться с помощью частотных словарей (для исключения широко употребляемых вариантов как "Qwerty", "ThisIsPassword" и т. д.) (если возможна реализация в ИС). Объем частотного словаря следует выбирать исходя из требования, что функционал проверки по частотному словарю не должен оказывать существенного негативного влияния на функционирование системы.

5.29. Пользователи обязаны обеспечивать хранение в тайне используемые ими пароли, не допускается разглашение или передача пользователями используемых паролей кому-либо. Нельзя сообщать, передавать кому-либо свой пароль. Пароли нельзя записывать на бумагу, в память телефона и т.д.

5.30. Пароли не должны храниться и передаваться в незашифрованном виде за пределы контролируемой зоны по публичным сетям (интернет, мессенджеры, электронная почта и т.д.).

5.31. Не допускается направление парольной информации, в т.ч. находящейся в зашифрованном контейнере (архиве), нескольким адресатам. Парольную информацию следует направлять только владельцу пароля. Парольную информацию от зашифрованного контейнера в таком случае необходимо передавать по другим каналам связи, другими способами, чем был передан зашифрованный контейнер.

5.32. Рекомендуется хранение паролей в зашифрованном виде в специальном ПО («Менеджерах паролей»).

5.33. Сброс пароля на временный технический для временно отсутствующего работника допускается при обращении руководителя подразделения работника.

5.34. Смена пароля сервисной или встроенной УЗ обязательна в случае увольнения или смены полномочий ответственного за формирование пароля.

5.35. При подозрении в компрометации пароля пользователь обязан произвести немедленную смену пароля и проинформировать ответственного за ИБ Учреждения.

5.36. Управление персонифицированными учетными записями работников (создание, активация, блокировка, удаление, изменение привилегий) осуществляется в соответствии с процессами управления персоналом (прием на

работу, перемещение, увольнение и др.) и отделом информационных технологий (например, в случае инцидента информационной безопасности).

5.37. Реквизиты доступа выдаются представителям подрядчика только на время действия договорных обязательств (выполнение работ, оказание услуг).

5.38. Использование одинаковых паролей администратора для различных сервисов или систем запрещено.

5.39. Действия, не требующие привилегий, не рекомендуется выполнять с использованием привилегированных учетных записей.

5.40. Допускается передача паролей администратора специалистам, которые задействованы в чрезвычайных ситуациях, с обязательной последующей заменой этих паролей.

5.41. Пароли административных учетных записей должны меняться после того, как у работника, который знает эти пароли, изменяются должностные обязанности или он увольняется.

5.42. Все службы и приложения должны запускаться от имени сервисных учетных записей. Использование для этих целей персонифицированных учетных записей запрещено.

5.43. В ИС должна быть настроена блокировка пользователей при неудачных попытках ввода пароля. Настроить временную блокировку доступа (если возможна реализация в ИС) к учетной записи после 5 неудачных попыток входа на 30 минут. После 10 неудачных попыток ввода пароля УЗ должна блокироваться перманентно. Разблокировка осуществляется через обращение к ответственному за ИБ. В случае невозможности реализации поэтапной/многоступенчатой блокировки, учетная запись должна блокироваться на время либо до ручной разблокировки.

5.44. После 10 минут бездействия доступ блокируется средствами системы и для разблокировки требуется введение пароля (пин-кода).

5.45. Удаленные сетевые сессии должны быть автоматически отключены не позднее чем через 30 минут бездействия пользователя.

5.46. Неактивные терминальные сессии автоматически должны закрываться по прошествии 60 минут.

6. Порядок управления доступом для работников Учреждения

6.1. Данный раздел определяет порядок выполнения следующих процедур:

- предоставление доступа пользователю;
- блокировка доступа пользователя;
- разблокировка доступа пользователя;
- удаление доступа (учетной записи) пользователя;

6.2. Участники (роли), задействованные в выполнении регламентируемых процедур, являются как должностными лицами, так и автоматизированными процедурами ИС (например, система контроля и управления доступом).

6.3. Ответственным за функционирование процесса предоставления доступа является ответственный за обеспечение ИБ в Учреждении. Обработку заявок по выдаче доступов реализуют работники отдела автоматизированной системы управления. Предоставление доступа и удаление учетной записи реализуется по согласованию ответственного за обеспечение ИБ в Учреждении.

6.4. Процедура предоставления доступа пользователю к ИС включает:

- предоставление доступов штатным работникам на основе согласованных матриц доступов (по возможности должно быть автоматизировано системой контроля и управления доступом);
- формирование заявки на доступ к ИС;
- согласование заявки на доступ к ИС;
- предоставление пользователю прав доступа в соответствии с заявкой;
- передачу идентификационной и аутентификационной информации пользователю для доступа к ИС;
- учет выполненной заявки.

6.5. Штатному работнику после трудоустройства создается УЗ в ИС системой контроля и управления доступов в соответствии с полномочиями, указанными в утвержденной руководителем работника матрице доступов для должности работника.

6.6. В случае отсутствия доступа в ИС или нехватки каких-либо полномочий руководитель работника или сам работник с резолюцией своего руководителя обращается к ответственному за администрирование.

6.7. Новый работник должен быть ознакомлен руководителем с Политикой ИБ, правилами доступа и ответственностью за невыполнение требований ИБ.

6.8. После предоставления прав доступа, пользователю безопасным способом передаются данные, необходимые для прохождения процедур идентификации и аутентификации при доступе к активам ИС.

Уровень доступа штатных работников структурных подразделений Учреждения предоставляются или актуализируются руководителями этих подразделений в адрес ответственного за обеспечение ИБ не реже 1 раза в год.

7. Порядок предоставления доступа Подрядчикам

7.1. Перед оформлением заявки на доступ Подрядчику, ответственный за действия Подрядчика должен согласовать и подписать Соглашение о конфиденциальности и неразглашении конфиденциальной информации (NDA).

7.2. Ответственный штатный работник Учреждения за действия Подрядчика (далее ответственный за действия Подрядчика) согласовывает предоставление доступа с ответственным за ИБ Учреждения.

7.3. В случае возникновения у Подрядчика необходимости привлечения для выполнения работ по договору дополнительных работников, ответственный за действия Подрядчика формирует заявку для создания УЗ с ранее утвержденными доступами и предоставляет список дополнительных Подрядчиков.

7.4. В случае, когда с Подрядчиком договорные отношения прекращаются ранее ожидаемого срока, ответственный за действия Подрядчика уведомляет об этом ответственного за ИБ Учреждения о блокировке доступа.

7.5. Все УЗ Подрядчиков создаются через систему контроля и управления доступом или соответствующую заявку. В случае отсутствия возможности предоставить полномочия через систему контроля и управления доступом, заявка передается администратору ИС, в которой предоставляется доступ.

7.6. После предоставления прав доступа ответственному за действия Подрядчика передаются необходимые данные УЗ для прохождения процедур идентификации и аутентификации при доступе к ИС.

7.7. Для работников компаний-партнеров применяется следующий алгоритм согласования доступа:

- доступ Подрядчику согласовывается с главным врачом и ответственным за ИБ Учреждения не реже 1 раза в год с приложением NDA, описанием проекта, оценкой рисков, назначением ответственного за действия Подрядчика со стороны Учреждения;
- в течение этого срока (не реже 1 раза в год) доступ отдельным специалистам Подрядчика предоставляется по заявке от руководителя структурного подразделения Учреждения согласно утвержденной матрице;
- любые изменения в матрице доступов согласовываются с ответственным за обеспечение ИБ (начальником отдела информационных технологий).

7.8. После выполнения заявка хранится в архиве заявок.

8. Требования к инвентаризации активов ИС

8.1. С целью контроля уровня безопасности для активов ИС Учреждения, их критичности по конфиденциальности, целостности, доступности и оперативного реагирования на инциденты информационной безопасности, уязвимости – активы ИС должны быть идентифицированы, описаны и за каждым активом должен быть закреплен ответственный работник Учреждения.

8.2. Для каждого актива ИС должен быть назначен владелец, который несет ответственность за реализацию, соблюдение, поддержание требований Политики, Стандарта и других правил информационной безопасности для технического сервиса, системы, за которые он ответственный.

8.3. Долже быть обеспечен контроль за работоспособностью, параметрами настройки и правильностью функционирования средств вычислительной техники, телекоммуникационного оборудования, системного программного обеспечения и средств защиты информации.

8.4. Все активы ИС Учреждения – технические сервисы, системы, сетевые устройства, автоматизированные рабочие места работников, серверы, базы данных, приложения должны быть идентифицированы и занесены в перечень (базу данных) активов технической инфраструктуры.

8.5. Перечень (база данных) активов технической инфраструктуры должна поддерживаться в актуальном состоянии.

8.6. Должен быть реализован автоматизированный контроль за составом и состоянием активов ИС.

9. Сервисы и системы в эксплуатации

9.1. Ввод новых сервисов и систем в эксплуатацию возможен только после выполнения требований настоящего Стандарта и дополнительных требований по информационной безопасности, которые были установлены в рамках жизненного цикла проекта.

9.2. Ответственность за соответствие сервиса, системы требованиям информационной безопасности возлагается на ответственного по ИБ.

10. Требования для устройств конечного пользователя

10.1. К устройствам конечного пользователя относятся автоматизированные рабочие места (АРМ) – рабочие ноутбуки, стационарные компьютеры работников Учреждения и мобильные технические средства (планшеты, смартфоны, если они используются для подключения к сервисам, системам Учреждения).

10.2. АРМ устанавливаются уполномоченными работниками Учреждения с предустановленным ПО, необходимым для выполнения служебных обязанностей.

10.3. Управление обновлениями должно вестись автоматически. Пользователи могут откладывать применение обновлений, но не отказываться от них.

10.4. Все предварительно настроенные учетные записи должны быть деактивированы, кроме тех, которые необходимы для управления и запуска

системных сервисов. Все активные учетные записи должны быть защищены механизмами аутентификации.

10.5. Все стандартные пароли учетных записей для систем и/или приложений, в использовании которых есть необходимость, должны быть изменены администратором перед вводом в эксплуатацию АРМ.

10.6. Все сетевые сервисы должны быть деактивированы, кроме тех, которые требуются для исполнения пользователем функциональных задач.

10.7. АРМ, подключаемое к сети Учреждения, должно иметь возможность быть идентифицированным в индивидуальном порядке с определением работника, ответственного за него.

10.8. Для каждого АРМ должна быть проведена процедура его авторизации (введение в домен MS AD) при подключении к внутренней сети Учреждения.

10.9. После того, как АРМ был авторизован в сети Учреждения, необходимо не реже одного раза в месяц подключать его к корпоративной сети для получения обновлений ОС, антивирусного ПО, доменных политик. Устройства, которые не соответствуют требованиям данного условия, через два месяца блокируются, затем удаляются из домена. Для получения доступа во внутреннюю сеть Учреждения необходимо заново пройти процедуру авторизации (повторное введение в домен).

10.10.АРМ должны иметь по крайней мере:

- актуальную версию ОС, поддерживаемую производителем;
- персональный межсетевой экран;
- антивирусное ПО с последними обновлениями;
- агента для управления устройством.

10.11.Доступ к сети Учреждения должен быть запрещен для АРМ, которое:

- не было должным образом авторизовано (например, не в домене);
- числится утерянным или украденным;
- не подключалось к сети Учреждения более двух месяцев;
- вовлечено в инцидент информационной безопасности.

10.12.АРМ, которые изымаются у существующего владельца, подлежат замене, ремонту внешними организациями, устаревают или выводятся из эксплуатации, должны быть возвращены в изначальное состояние с обязательным удалением всей информации без возможности ее восстановления прежде, чем будут переданы следующему владельцу.

10.13.Для минимизации рисков, связанных с успешным заражением вредоносным ПО, успешной кибератакой на АРМ, по умолчанию работник не имеет прав локального администратора на АРМ.

10.14.Права локального администратора на АРМ могут предоставляться только в случае обоснованной необходимости на время проведения работ. Предоставление таких прав возможно для работников Учреждения, обслуживающих критичные сервисы и системы, перебои в работе которых приводят к неработоспособности сети, влияют на обслуживание клиентов и взаимодействие с партнерами.

10.15.Локальным администраторам запрещается:

- устанавливать, модифицировать и/или удалять любое ПО;
- добавлять или удалять любые учетные записи;
- изменять системные параметры;
- изменять сетевые параметры (при этом, в случае служебной необходимости, сетевые параметры могут быть изменены).

10.16. Ответственный за обеспечение ИБ должен осуществлять мониторинг пользователей с правами локальных администраторов и иметь право санкционировать их отзыв.

10.17.Мобильные технические средства должны иметь возможность быть идентифицированным при подключении к активам ИС Учреждения в индивидуальном порядке с определением работника, ответственного за него.

10.18.При подключении к активам ИС Учреждения с мобильных технических средств должны выполняться, как минимум, следующие требования:

- актуальная версия ОС, поддерживаемая производителем;
- антивирусное ПО с последними обновлениями;
- использоваться принудительный механизм блокировки, который предотвращает неавторизованное использование мобильного технического средства (пин-код или проверка биометрических данных (например, идентификация отпечатка пальца, Face ID и т.д.));
- отсутствие несанкционированных производителем изменений в операционной системе мобильного устройства (jail-break, unlock, root);
- использование механизма двухфакторной аутентификации при доступе к сервисам, системам, информации Учреждения.

10.19.Должна обеспечиваться физическая защита мобильных технических средств конечных пользователей от кражи (например, в автомобилях и других видах транспорта, в гостиничных номерах, конференц-центрах и местах проведения совещаний).

11. Требования к управлению программным обеспечением

11.1. Должен быть определен перечень разрешенного программного обеспечения и регламентация порядка его установки и использования с учетом рабочих процессов в Учреждении.

11.2. Копирование ПО с АРМ работника либо из репозитория на личный компьютер запрещено.

11.3. Должно быть обеспеченно своевременное обновление программного обеспечения за исключением случаев, влекущих прекращение функционирования этих активов.

11.4. На всех активах ИС должны быть установлены обновления безопасности (при наличии).

11.5. Плановая проверка наличия обновлений активов ИС должно проводиться не реже одного раза в месяц.

12. Защита от вредоносного программного обеспечения

12.1. Антивирусное программное обеспечение должно быть на каждом АРМ и на каждом сервере под управлением ОС Windows. Защита от вредоносного ПО для других типов ОС (например ОС Linux) определяется в рамках анализа подверженности воздействию вредоносному ПО.

12.2. Автоматизированной проверке с помощью антивирусного программного обеспечения подлежат:

- АРМ работников Учреждения;
- серверы под управлением ОС Windows;
- съемные носители информации.
- весь входящий почтовый трафик;
- весь входящий, исходящий веб-трафик при доступе работников или серверов в сеть Интернет.

12.3. В Учреждении должны использоваться только лицензионные версии антивирусного программного обеспечения, имеющие сертификат соответствия на требования Технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY).

12.4. Антивирусное программное обеспечение должно поддерживаться производителем и получать актуальные сигнатуры.

12.5. Обновление антивирусных баз должно происходить автоматически без вмешательства администраторов.

12.6. Антивирусное программное обеспечение должно быть настроено на автоматическое получение и установку обновлений. Данные обновления должны применяться не позже, чем в течение 24 часов после их получения.

12.7. Антивирусное программное обеспечение должно поддерживать следующие режимы работы: защита от вредоносного программного обеспечения в режиме реального времени, периодическое сканирование по расписанию.

12.8. Периодическое сканирование по расписанию должно проводиться не реже одного раза в неделю.

12.9. Антивирусное программное обеспечение должно генерировать журналы протоколирования событий и отправлять их на центральный сервер протоколирования событий.

12.10. Рекомендуется использование решений класса Endpoint Detection and Response (EDR), которые ведут непрерывный мониторинг, собирают и коррелируют данные с конечных точек в режиме реального времени для выявления подозрительную активность на хостах и конечных точках и принятия ответных действий.

13. Использование съемных носителей информации

13.1. К съемным носителям информации относятся носители, которые могут быть подключены к вычислительным системам с использованием штатных портов (USB и т.п.), расположенных на внешних поверхностях корпуса. К ним относятся накопители на основе флеш-памяти, оптические CD/DVD/BD диски, внешние жесткие диски, твердотельные накопители с энергозависимой памятью и т.п.

13.2. Должен производиться учет съемных носителей информации, содержащих информацию ограниченного распространения.

13.3. Хранение носителей информации должно осуществляться в безопасных условиях в соответствии с их информационной классификацией и защитой их от угроз окружающей среды (таких как тепло, вода, влажность, электронное поле или старение) в соответствии со спецификациями производителей.

13.4. Если конфиденциальность или целостность информации являются важными факторами, должны использоваться криптографические методы защиты информации на съемных носителях информации.

13.5. Для снижения риска деградации носителя, когда хранимая информация еще необходима, должен осуществляться перенос информации на свежий носитель до того, как она станет нечитаемой.

13.6. Рекомендуется применять хранение нескольких копий ценной информации на отдельных носителях для дополнительного снижения риска случайного повреждения или потери информации.

13.7. Носители информации должны быть защищены от несанкционированного доступа, ненадлежащего использования или повреждения во время транспортирования или отправки по почте.

13.8. Для уничтожения данных может применяться программное обеспечение, производящее перезапись данных всего носителя случайными данными.

13.9. В случае, когда носитель информации приходит в негодность, или, когда его хранение является нецелесообразным, он должен уничтожаться.

13.10.Для уничтожения носителей информации на основе флеш-памяти и твердотельных накопителей с энергозависимой памятью необходимо испортить микросхему накопителя путем физического воздействия (удар молотком и т.п.).

13.11.Для уничтожения оптических дисков необходимо испортить рабочую сторону диска путем трения наждачной бумагой или ломкой/резкой диска на мелкие части или с помощью специального оборудования для уничтожения компакт-дисков.

14. Электронная почта

14.1. Рабочая электронная почта является одним из видов деловых коммуникаций и одним из сервисов, предоставляемых Учреждением своим работникам.

14.2. Электронные письма отправляются только тем лицам, которым содержащаяся в них информация необходима для выполнения служебных задач. Следует избегать избыточных списков адресатов, перегружающих множество получателей ненужной информацией, отвлекающей их от работы.

14.3. Электронные письма сохраняются на почтовом сервере, который предоставляется ООО «Белорусские облачные технологии».

14.4. Работник Учреждения может сохранять необходимые электронные письма в течение более продолжительного срока (например, в виде *.pst файлов) с использованием сетевых ресурсов, выделенных для его подразделения, либо на АРМ.

14.5. Пользователь рабочей электронной почты (работник Учреждения) при отправке сообщений внешним пользователям (корреспондентам) выступает в роли представителя Учреждения, что налагает на него особую ответственность.

14.6. При работе с электронной почтой следует знать, что периодически на рабочие ящики работников могут приходить нежелательные, вредоносные письма. Такие письма могут содержать различные вирусы и вредоносные программы во вложении, либо содержать ссылки на ресурсы, где расположены вредоносные программы или созданы специальные фейк-сайты для сбора учетных записей, паролей со стороны злоумышленников.

14.7. Как правило, вредоносные письма направлены на заражение АРМ, захвата паролей учетных записей с целью их компрометации и создания предпосылок к взлому активов Учреждения, что может привести к нарушению конфиденциальности, целостности, доступности информации, а значит нанести материальный, репутационный ущерб Учреждению.

14.8. Например, пройдя по ссылке из такого вредоносного письма или открыв вложение, АРМ может быть заражено, а так как оно имеет доступ к активам Учреждения, заражение может распространиться по сети, что даст

злоумышленнику возможность провести следующие стадии кибератаки на активы ИС.

14.9. При получении вредоносных писем, важно их идентифицировать и правильно своевременно на них отреагировать. Правила идентификации и реагирования со стороны работников Учреждения описаны в разделе «Инциденты информационной безопасности» настоящего документа.

14.10.Адреса электронной почты, предоставленные всем работникам Учреждения, предназначены для использования только в служебных целях. Недопустимо использование рабочего почтового адреса для целей, не связанных с выполнением служебных обязанностей (например, регистрация в интернет-магазинах и иных онлайн сервисах).

14.11.Учреждение имеет право доступа к электронному служебному почтовому ящику работника в следующих случаях:

- при отсутствии владельца почтового ящика лицо, его замещающее либо иное уполномоченное лицо может получить доступ к его электронным письмам только в связи со служебной необходимостью;
- если имеется обоснованное подозрение работника в незаконных действиях или уголовном преступлении в порядке, определенном законодательством Республики Беларусь и/или трудовым договором (контрактом).

15. Синхронизация времени

15.1. Для всех активов ИС системные часы должны быть синхронизированы с единым источником информации о точном времени в ИС.

15.2. Единый источник информации о точном времени должен получать информацию о точном времени из доверенного внешнего источника.

15.3. Архитектура синхронизации времени активов ИС должна быть задокументирована.

16. Протоколирование событий

16.1. Для каждого актива ИС, в которых хранится, обрабатывается или через которые передается защищаемая информация, должно выполняться протоколирование событий информационной безопасности (далее - события). При этом события должны храниться в локальных журналах активов ИС не менее одного года с целью возможности расследования инцидентов информационной безопасности.

16.2. В целях обеспечения реализации мониторинга и управления инцидентами информационной безопасности, протоколированию в сервисах и системах на всех уровнях должны подлежать, как минимум следующие события:

- использование и изменение механизмов идентификации,
  аутентификации, авторизации (успешный, неуспешный вход, выход;

повышение привилегий; изменение прав доступа учетных записей; создание/изменение/блокировка/удаление учетных записей; сброс пароля и т.д.);

- любой доступ к журналам событий;
- очистка журналов событий;
- остановка или отключение записи логов;
- создание, удаление, изменение объектов сервиса, системы;
- изменение конфигураций, настроек;
- кибератаки и вредоносная активность, аномалии в отношении активов ИС (как правило события, генерируемые средствами защиты информации).

16.3. Как минимум события должны содержать следующую информацию:

- время, дата возникновения;
- совершенное действие;
- инициатор действия;
- имена ресурсов, IP адрес(а);
- имена учетных записей;
- сервис, система, приложение.

16.4. Для части активов (например, межсетевые экраны, антиспам, прокси, IDS/IPS, антивирус, иные средства защиты информации), которые предоставляют релевантные и качественные данные для мониторинга вредоносной активности в ИС Учреждения, журналы протоколирования событий должны направляться и храниться в централизованном хранилище. Срок централизованного хранения должен составлять не менее 1 года.

16.5. При централизованном хранении в SIEM журналов событий активов ИС, на этих активах журналы событий должны храниться и быть доступными локально за последние два дня.

16.6. Факты подключения представителей внешних организаций протоколируются и хранятся не менее года.

16.7. Должен быть определен способ (просмотр, анализ) и периодичность мониторинга событий информационной безопасности уполномоченными на это пользователями ИС.

16.8. Доступ к журналам протоколирования событий должен быть ограничен в соответствии с принципами наименьших привилегий и рабочей необходимости.

17. Инциденты информационной безопасности

17.1. Мониторинг информационной безопасности состоит из следующих стадий:

- планирование мониторинга;

- осуществление мониторинга.

17.2. В ходе мониторинга должны анализироваться события информационной безопасности, с целью выявления угроз, которые могут привести к сбоям, нарушению функционирования активов ИС. События информационной безопасности должны анализироваться на регулярной основе.

17.3. Источниками событий безопасности могут являться журналы протоколирования событий, а также зарегистрированные обращения работников Учреждения и третьих лиц.

17.4. В случае подозрений на инциденты информационной безопасности работники Учреждения должны обращаться к ответственному за обеспечение ИБ в Учреждении.

17.5. Если в ходе анализа было установлено, что событие безопасности является инцидентом, необходимо зарегистрировать инцидент. Все инциденты информационной безопасности должны быть зарегистрированы.

17.6. После получения информации об инциденте необходимо незамедлительно принять меры по устранению негативных последствий инцидента для Учреждения.

17.7. Все обнаруженные инциденты должны быть расследованы в целях выяснения причин возникновения инцидента и недопущения повторения аналогичных инцидентов в будущем.

18. Криптографическая защита

18.1. Криптографическая защита информации в Учреждении должна применяться:

- при организации удаленного пользовательского и административного доступа к активам ИС;
- для защиты резервных копий данных (виртуальных машин);
- для защиты информации, хранимой на переносных или сменных носителях и устройствах;
- для защиты информации, передаваемой в сетях электросвязи общего пользования;
- для защиты аутентификационных данных (например, паролей).

18.2. В процессе эксплуатации средств криптографической защиты информации должны быть организованы и поддерживаться меры, обеспечивающие особый режим допуска на территорию (в помещения), на которой может быть осуществлен доступ к криптографическим средствам и ключам (носителям).

18.3. Криптографическая архитектура решений по защите резервных копий виртуальных машин, решений по защите удаленного пользовательского и

административного доступа к техническим сервисам и системам, а также решений по защите данных, хранимых на носителях и передаваемых в общедоступной сети, должна быть задокументирована.

18.4. Для получения административного доступа к активам ИС должны использоваться только стойкие криптографические алгоритмы и протоколы, обеспечивающие шифрование информации. На активах ИС должны быть отключены небезопасные протоколы, не поддерживающие шифрование информации (например, telnet, http).

18.5. При получении пользовательского и административного доступа к активам ИС по протоколу HTTPS следует убедиться, что для шифрования трафика используется протокол TLS не ниже версии 1.2. TLS-сертификаты должны быть выпущены внутренним центром цифровых сертификатов (удостоверяющим центром) Учреждения или доверенным внешним центром цифровых сертификатов.

18.6. При получении административного доступа по протоколу SSH должна использоваться 2-ая версия протокола.

18.7. При передаче информации сетях электросвязи общего пользования данные должны шифроваться с использованием средств линейного (сетевого) шифрования.

18.8. При организации криптографической защиты должны применяться стойкие протоколы, криптографические алгоритмы, длины ключей.

18.9. Длины ключей криптографических алгоритмов, являющиеся государственными стандартами Республики Беларусь, установлены в соответствующих стандартах.

18.10.Все криптографические ключи следует защищать от модификации и потери. Кроме того, секретные и личные ключи нуждаются в защите от неавторизованного использования и раскрытия. Следует, чтобы оборудование (при наличии), используемое для генерации, хранения и архивации ключей, было физически защищено.

18.11.При использовании средств электронной цифровой подписи для взаимодействия с внешними информационными системами должны быть обеспечены конфиденциальности и контроля целостности личных ключей (например, использование криптографического токена).

19. Удаленный доступ

19.1. Удаленный доступ предоставляется в соответствии с принципами рабочей необходимости и наименьших привилегий (должен быть ограничен минимальным количеством активов ИС, портов, сетевых сервисов и минимальным уровнем прав доступа).

19.2. Удаленный доступ для работников Учреждения допускается только с контролируемых политиками безопасности Учреждения устройств (АРМ).

19.3. При организации удаленного доступа для внешних организаций должна быть обеспечена защита от:

- несанкционированных изменений в сервисе, системе;
- вредоносной активности (заражение вредоносным ПО) в отношении активов ИС;
- утечки информации.

19.4. Для организации защиты могут использоваться промежуточные терминальные серверы с преднастроенными политиками безопасности.

19.5. При необходимости организации непрерывного соединения между сетью Учреждения и сетью внешней организации, требуется построение шифрованного туннеля между объектами с применением СКЗИ.

20. Исключения

20.1. Исключения из руководящих принципов, требований данного Стандарта могут быть выполнены для частных случаев, если есть веская обоснованная причина невозможности соответствия требованиям Стандарта.

20.2. Для каждого потенциального частного исключения должен проводиться анализ рисков информационной безопасности, выдвигаться предложения по компенсационным мерам, если таковые возможно применить.

21. Правовые требования и последствия

21.1. С целью минимизации возможного ущерба из-за несоблюдения требований настоящего Стандарта уполномоченные должностные лица обязаны создать условия, позволяющие обеспечить соблюдение установленных мер обеспечения информационной безопасности и осуществлять контроль их выполнения.

21.2. Лица, виновные в нарушении положений данного Стандарта, могут быть привлечены к ответственности в соответствии с законодательством Республики Беларусь и локальными правовыми актами Учреждения.

22. Ответственность

22.1. Руководство Учреждения придерживается требований настоящего документа в ходе осуществлении служебной деятельности.

22.2. Руководство Учреждения и руководители подразделений, которые являются ответственными за поддержу, эксплуатацию, развитие ИС Учреждения, обеспечивают уровень информационной безопасности, установленный настоящим Стандартом.

22.3. Руководство Учреждения должно организовать на регулярной основе, но не реже одного раза в год, проведение:

- инструктажей, иных мероприятий, направленных на повышение уровня знаний и навыков работников Учреждения по вопросам применения системы защиты информации в части, их касающейся;
- анализа эффективности применения системы защиты информации, включая пересмотр применяемых мер по защите информации на предмет их актуальности и необходимости внесения изменений в систему защиты информации.

ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ, СОКРАЩЕНИЯ

Термин, определение, сокращение	Пояснение
Авторизация	предоставление субъекту доступа прав доступа, а также предоставление доступа в соответствии с установленными правилами управления доступом (предоставление определённому пользователю (учетной записи) определенных прав доступа в ИС на выполнение определённых действий, а также процесс проверки (подтверждения) данных прав при попытке выполнения этих действий). Примечание: положительный результат идентификации и аутентификации является одним из оснований для авторизации субъекта доступа.
Администратор	работник, в должностные (трудовые) обязанности которого входят функции администрирования в определенной ИС.
Активы информационной системы	средства вычислительной техники, телекоммуникационное оборудование, системное и прикладное программное обеспечение, информационные ресурсы, входящие в состав информационной системы.
АРМ	автоматизированное рабочее место.
Аутентификация	обеспечение однозначного соответствия заявленного идентификатора объекту.
Владелец актива ИС	субъект, осуществляющий владение и пользование средствами вычислительной техники, телекоммуникационного оборудования, системного и прикладного программного обеспечения, информационными ресурсами и реализующий полномочия распоряжения в пределах, установленных собственником (ответственный за определение круга лиц, имеющих доступ к информационному ресурсу, а также за период использования информационного ресурса).
ИБ	информационная безопасность - состояние защищенности активов информационной системы

	от угроз и рисков информационной безопасности информационной системы.
Идентификация	процесс присвоения объекту уникального идентификатора. Примечание: процесс идентификации в общем случае предусматривает последующие аутентификацию, авторизацию и доступ.
Инцидент информационной безопасности (киберинцидент)	событие, которое фактически или потенциально угрожает конфиденциальности, целостности, подлинности, доступности и сохранности информации, а также представляет собой нарушение (угрозу нарушения) политики безопасности.
ИС	Информационная система и/или сервис. Прикладная система, база данных, сетевой сервис, доступ к которым ограничен средствами управления доступом.
Контроль прав доступа	систематическая проверка соответствия полномочий работников в ИС их роли, выявляет полномочия/учетные записи, присвоенные/созданные в обход системы контроля и управления доступом.
Матрица доступа	таблица, описывающая права доступа субъектов к объектам доступа.
Несанкционированный доступ к информации	доступ к информации, осуществляемый с нарушением установленных прав или правил разграничения доступа.
Учреждение	учреждение здравоохранения «Гомельская городская клиническая больница № 2».
Права доступа	официально полученная возможность доступа к определенным функциям ИС.
ПО	программное обеспечение.
Роль	это набор полномочий, который необходим пользователю или группе пользователей для выполнения определённых рабочих задач. Каждый работник может иметь одну или несколько ролей, а каждая роль может содержать от одного до

	множества полномочий, которые разрешены пользователю в рамках этой роли. Роли могут быть привязаны к определённым должностям, подразделениям или функциональным задачам работников. Роль может быть автоматизирована в ИС.
Учетная запись (УЗ)	запись, содержащая сведения, необходимые для идентификации пользователя при подключении к системе, информацию для аутентификации, авторизации и учёта.
NDA	Соглашение о конфиденциальности и неразглашении конфиденциальной информации.