МІНІСТЭРСТВА АХОВЫ ЗДАРОЎЯ РЭСПУБЛІКІ БЕЛАРУСЬ

ЗАГАД

19.11.2019 № 1115

г. Мінск

МИНИСТЕРСТВО ЗДРАВООХРАНЕНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

ПРИКАЗ

г. Минск

О вопросах обеспечения информационной безопасности в здравоохранении

На основании абзаца восемнадцатого части третьей статьи 8 Закона Республики Беларусь от 18 июня 1993 г. № 2435-XII «О здравоохранении» и подпункта 9.1 пункта 9 Положения о Министерстве здравоохранения Республики Беларусь, утвержденного постановлением Совета Министров Республики Беларусь от 28 октября 2011 г. № 1446,
ПРИКАЗЫВАЮ:

1. Утвердить Концепцию информационной безопасности здравоохранения (прилагается).

2. Пункт 8 приложения 1 к приказу Министерства здравоохранения Республики Беларусь от 26 сентября 2018 г. № 959 «О распределении обязанностей между руководством Министерства здравоохранения Республики Беларусь и курации областей Республики Беларусь» дополнить подпунктом 8.24 следующего содержания:

«8.24. координирует и организует внедрение мер по обеспечению информационной безопасности здравоохранения.».

3. Определить государственное учреждение «Республиканский научно-практический центр медицинских технологий, информатизации, управления и экономики здравоохранения» (далее – РНПЦ МТ) (отдел по обеспечению информационной безопасности) ответственным подразделением информационной безопасности здравоохранения.

4. Директору РНПЦ МТ Сачек М.М. в срок до 30 января 2020 г. внести для утверждения (согласования):

План реализации положений Концепции информационной безопасности здравоохранения;

Положение об ответственном подразделении информационной безопасности здравоохранения;

Типовое положение о должностном лице, ответственном за информационную безопасность (подразделении по обеспечению информационной безопасности организации здравоохранения) в главных

РИЦ. Зак. 97. Тир. 2000. 2019

управлениях по здравоохранению облисполкомов, комитете по здравоохранению Минского горисполкома и в организациях здравоохранения.

5. Начальникам главных управлений по здравоохранению облисполкомов, председателю комитета по здравоохранению Минского горисполкома, руководителям государственных организаций, подчиненных Министерству здравоохранению:

5.1. до 20 февраля 2020 г. разработать и утвердить Положение о должностном лице, ответственном за информационную безопасность (подразделении по обеспечению информационной безопасности организации здравоохранения) в соответствии с Типовым положением о должностном лице, ответственном за информационную безопасность (подразделении по обеспечению информационной безопасности организации здравоохранения) в главных управлениях по здравоохранению облисполкомов, комитете по здравоохранению Минского горисполкома и в организациях здравоохранения;

5.2. до 20 февраля 2020 г. назначить должностных лиц, ответственных за информационную безопасность.

Копии приказов о назначении должностных лиц, ответственных за информационную безопасность в главных управлениях здравоохранения облисполкомов, комитете по здравоохранению Минского горисполкома, государственных организациях, подчиненных Министерству здравоохранения, направить в отдел по обеспечению информационной безопасности РНПЦ МТ;

5.3. организовать повышение квалификации назначенных должностных лиц по программам курсов «Основы безопасности информационных технологий» и (или) «Безопасность информационных технологий» в порядке, установленном законодательством.

Копии свидетельств государственного образца о повышении квалификации и переподготовке кадров направить в отдел по обеспечению информационной безопасности РНПЦ МТ.

6. Контроль исполнения настоящего приказа возложить на первого заместителя Министра здравоохранения Пиневича Д.Л.

Министр — В.С.Караник

УТВЕРЖДЕНО

приказ
Министерства здравоохранения
Республики Беларусь
29.11.2019 № 1115

КОНЦЕПЦИЯ
информационной безопасности здравоохранения

РАЗДЕЛ I
ОБЩИЕ ПОЛОЖЕНИЯ

ГЛАВА 1
ОБОСНОВАНИЕ РАЗРАБОТКИ КОНЦЕПЦИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЗДРАВООХРАНЕНИЯ

1. Необходимость разработки Концепции информационной безопасности здравоохранения обусловлена расширением сферы применения новейших информационных технологий и процессов при обработке информации.

В организациях здравоохранения обрабатываются значительные объемы конфиденциальной информации, содержащей как персональные данные работников отрасли и пациентов, так и сведения, составляющие врачебную тайну, что, в свою очередь, делает необходимым обеспечение высокого уровня информационной безопасности.

В настоящее время в Республике Беларусь проходит активная информатизация здравоохранения, обозначен плановый переход к комплексной автоматизации медицинской деятельности, объединению разнородных медицинских информационных систем в единое информационное пространство, внедрению технологий электронной записи на прием к врачу, электронных медицинских карт пациента, электронного рецепта и других.

Автоматизация деятельности организаций здравоохранения приводит к появлению новых уязвимостей и угроз и, как следствие, новых рисков информационной безопасности не только для организаций здравоохранения, но и для пациентов.

Таким образом, особое внимание при внедрении процессов информатизации и автоматизации здравоохранения должно уделяться обеспечению информационной безопасности и защите информации.

ГЛАВА 2
ОСНОВНЫЕ ПОЛОЖЕНИЯ КОНЦЕПЦИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЗДРАВООХРАНЕНИЯ

2. Концепция информационной безопасности здравоохранения (далее – Концепция) определяет основные цели и задачи, а также общую стратегию и направление деятельности по обеспечению информационной безопасности в здравоохранении.

3. Концепция разработана в соответствии с системным подходом к обеспечению информационной безопасности, который предполагает проведение комплекса мероприятий, включающих исследование угроз информационной. безопасности и создание систем защиты информации с позиции комплексного применения технических, организационных мер и средств защиты.

4. Концепция является методологической основой для:

формирования и проведения единой политики в области обеспечения информационной безопасности здравоохранения;

принятия управленческих решений и разработке практических мер по воплощению политики безопасности, выработке комплекса согласованных мер нормативно-правового, технологического и организационно-технического характера, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз;

координации деятельности Министерства здравоохранения Республики Беларусь, главных управлений по здравоохранению облисполкомов, комитета по здравоохранению Минского горисполкома, организаций здравоохранения при проведении работ по развитию и эксплуатации информационных систем с соблюдением требований обеспечения безопасности информации;

разработки предложений по совершенствованию правовых, нормативных, методических, технических и организационных мер, направленных на обеспечение безопасности информации.

5. Положения Концепции развиваются нормативными правовыми актами Министерства здравоохранения Республики Беларусь, которые дополняют и уточняют ее.

6. Положения Концепции должны быть использованы для определения политики информационной безопасности в организациях здравоохранения. При формировании политики информационной безопасности в организациях здравоохранения отдельные положения настоящей Концепции требуют уточнения.

ГЛАВА 3
ОБЛАСТЬ ПРИМЕНЕНИЯ

7. Действие Концепции распространяется на:

центральный аппарат Министерства здравоохранения Республики Беларусь;

главные управления здравоохранения облисполкомов, комитет по здравоохранению Минского горисполкома;

организации здравоохранения, эксплуатирующие технические и программные средства информационных систем, в которых осуществляется автоматизированная обработка информации ограниченного распространения;

организации здравоохранения, разрабатывающие и сопровождающие программные и технические средства информационных систем.

ГЛАВА 4
ПРАВОВАЯ ОСНОВА РАЗРАБОТКИ КОНЦЕПЦИИ

8. Правовой основой для разработки настоящей Концепции являются требования нормативных правовых актов:

Концепция информационной безопасности Республики Беларусь, утвержденная постановлением Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1 «О Концепции информационной безопасности Республики Беларусь»;

Закон Республики Беларусь от 18 июня 1993 г. № 2435-XII «О здравоохранении»;

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

Закон Республики Беларусь от 28 декабря 2009 г. № 113-З «Об электронном документе и электронной цифровой подписи»;

Указ Президента Республики Беларусь от 16 апреля 2013 г. № 196 «О некоторых мерах по совершенствованию защиты информации»;

постановление Совета Министров Республики Беларусь от 26 мая 2009 г. № 673 «О некоторых мерах по реализации Закона Республики Беларусь «Об информации, информатизации и защите информации» и о признании утратившими силу некоторых постановлений Совета Министров Республики Беларусь»;

приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 30 августа 2013 г. № 62 «О некоторых вопросах технической и криптографической защиты информации» (в редакции

приказа Оперативно-аналитического центра при Президенте Республики Беларусь от 11 октября 2017 г. № 64),

а также международные нормативные правовые акты, ратифицированные в установленном порядке, в том числе международные технические нормативные акты, и технические нормативные правовые акты Республики Беларусь, содержащие положения по обеспечению безопасности информации.

ГЛАВА 5
ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

9. В документе используются термины, определенные в:

Концепции информационной безопасности Республики Беларусь, утвержденной постановлением Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1;

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

Законе Республики Беларусь от 18 июня 1993 г. № 2435-XII «О здравоохранении»;

СТБ ISO/IEC 27000-2012 «Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Основные положения и словарь»;

СТБ 34.101.1-2014 (ISO/IEC 15408-1:2009) «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель».

ГЛАВА 6
СОКРАЩЕНИЯ

10. В документе используются следующие сокращения:

ГО	-	государственная организация, подчиненная Министерству здравоохранения;
ИБ	–	информационная безопасность;
ИС	–	информационная система;
ИТ	–	информационная технология;
ЛНПА	–	локальный нормативный правовой акт;
Минздрав	–	Министерство здравоохранения Республики Беларусь;
МИС	–	медицинская информационная система;
НПА	–	нормативный правовой акт;
ОАЦ	–	Оперативно-аналитический центр при Президенте Республики Беларусь;

ОЗ	–	организация здравоохранения;
ПО	–	программное обеспечение;
СВТ	–	средство вычислительной техники;
СЗИ	–	система защиты информации;
СУИБ	–	система управления информационной безопасностью;
ЦА Минздрава	–	центральный аппарат Министерства здравоохранения Республики Беларусь;
DoS	–	Denial of Service (атака «Отказ в обслуживании»);
DDoS	–	Distributed Denial of Service (распределенная атака «отказ в обслуживании»).

РАЗДЕЛ II
ЦЕЛИ И ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЗДРАВООХРАНЕНИИ

ГЛАВА 7
ЦЕЛИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

11. Основными целями обеспечения ИБ в здравоохранениИ является:

обеспечение основных свойств защищаемой информации: конфиденциальности, целостности, доступности;

минимизация ущерба от возможной реализации угроз безопасности информации.

ГЛАВА 8
ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

12. Обеспечение ИБ здравоохранения должно осуществляться в соответствии со следующими принципами:

принцип законности, который предполагает осуществление мероприятий по обеспечению ИБ в соответствии с законодательством, регулирующим вопросы обеспечения ИБ и защиты информации;

принцип системности, который предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения ИБ;

принцип комплексности, который предполагает комплексное использование методов и средств защиты. Комплексный подход предполагает согласованное применение разнородных средств защиты информации при построении целостной СЗИ, перекрывающей все

существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных компонентов;

принцип непрерывности, который предполагает принятие соответствующих мер на всех этапах жизненного цикла ИС;

принцип своевременности, который предполагает упреждающий характер мер обеспечения безопасности данных, то есть постановку задач по комплексной защите ИС и реализацию мер обеспечения безопасности данных на ранних стадиях разработки ИС в целом и ее системы защиты информации в частности. Разработка системы защиты ведётся параллельно с разработкой и развитием самой защищаемой системы. Это позволяет учитывать требования безопасности при проектировании архитектуры и, в конечном счете, создать более эффективные (как по затратам ресурсов, так и по стойкости) защищенные системы;

принцип преемственности и совершенствования, который предполагает постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования ИС и ее СЗИ с учетом изменений в методах и средствах перехвата информации, требований НПА по обеспечению безопасности информации, достигнутого отечественного и зарубежного опыта в этой области;

принцип персональной ответственности, который предполагает возложение ответственности за обеспечение безопасности информации и системы их обработки на каждого пользователя МИС ОЗ в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей пользователей МИС ОЗ строится таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму;

принцип минимизации полномочий, который означает предоставление пользователям минимальных прав доступа в соответствии с необходимостью, на основе принципа «все, что не разрешено, запрещено». Доступ к ресурсам должен предоставляться только в том случае и объеме, если это необходимо пользователю МИС для выполнения его должностных обязанностей;

принцип взаимодействия и сотрудничества, который предполагает создание благоприятной атмосферы в коллективах Минздрава и ОЗ, обеспечивающих эксплуатацию МИС, для снижения вероятности возникновения негативных действий, связанных с человеческим фактором;

принцип гибкости системы обеспечения безопасности информации, который предполагает возможность изменения уровня защищенности МИС в зависимости от принятых мер и используемых средств защиты.

Это особенно важно в начальный период эксплуатации МИС, когда может обеспечиваться как чрезмерный, так и недостаточный уровень защиты, а также в случае установки средств защиты на работающую МИС без нарушения процесса ее нормального функционирования;

принцип открытости алгоритмов и механизмов защиты, который предполагает, что защита не должна обеспечиваться только за счет конфиденциальности структуры и алгоритмов функционирования ее подсистем. Знание алгоритмов работы СЗИ не должно давать возможности ее преодоления (даже разработчикам). Однако, это не означает, что информация о конкретной СЗИ должна быть общедоступна;

принцип научной обоснованности и технической реализуемости, который предполагает использование информационных технологий, технических и программных средств, средств и мер защиты информации, реализованных на современном уровне развития науки и техники, научно обоснованных с точки зрения достижения заданного уровня безопасности информации, и соответствующих установленным нормам и требованиям обеспечения безопасности информации. СЗИ должна быть ориентирована на такие решения, возможные риски для которых и меры противодействия этим рискам прошли всестороннюю теоретическую и практическую проверку;

принцип специализации и профессионализма, который предполагает привлечение к разработке средств и реализации мер защиты информации специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности данных, имеющих опыт практической работы и специальное разрешение (лицензию) на право оказания услуг по технической и криптографической защите информации, выданной ОАЦ;

принцип обязательности контроля, который предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности данных на основе используемых систем и средств защиты информации при совершенствовании критериев и методов оценки эффективности этих систем и средств. Контроль деятельности любого пользователя, каждого средства защиты и в отношении любого объекта защиты должен осуществляться на основе применения средств оперативного контроля и регистрации и должен охватывать как несанкционированные, так и санкционированные действия пользователей.

РАЗДЕЛ III
ОСНОВНЫЕ АКТИВЫ, ПОДЛЕЖАЩИЕ ЗАЩИТЕ. МОДЕЛИ НАРУШИТЕЛЕЙ И УГРОЗ

ГЛАВА 9
ОСНОВНЫЕ АКТИВЫ, ПОДЛЕЖАЩИЕ ЗАЩИТЕ

13. Основные активы, подлежащие защите, подразделяются на два вида:

базовые, к которым относятся процессы и информация;

вспомогательные (поддерживающие) активы.

14. К базовым активам, подлежащим защите относятся:

основная и вспомогательная деятельность организаций, входящих в структуру здравоохранения, включающая:

процессы, утрата или ухудшение качества которых делает невозможным выполнение целевой задачи ОЗ;

процессы, созданные с использованием высокоуровневых технологий;

процессы, модификация которых может значительно повлиять на реализацию назначения ОЗ;

процессы, которые необходимы ОЗ для выполнения договорных, правовых или регулирующих требований;

информационные ресурсы, независимо от формы и вида их представления, содержащие врачебную тайну, персональные данные физических лиц, сведения, составляющие служебную информацию ограниченного распространения (при ее наличии), а также информация, распространение и (или) предоставление которой не ограничено, необходимая для работы здравоохранения в целом;

информационные ресурсы, независимо от формы и вида их представления, содержащие врачебную тайну, персональные данные физических лиц, сведения, составляющие служебную информацию ограниченного распространения (при ее наличии), а также информация, распространение и (или) предоставление которой не ограничено, необходимая для работы каждой ОЗ;

стратегическая информация, содержащая сведения, необходимые для достижения целей, определяемых стратегией развития здравоохранения в целом и каждой ОЗ.

15. К вспомогательным (поддерживающим) активам, подлежащим защите, относятся:

ИТ-инфраструктура, включающая:

прикладное и системное ПО;

системы обработки и анализа информации;

сервисы общего назначения и сервисы конечного пользователя;

технические и программные средства хранения, обработки, передачи и отображения информации;

электронные (flash-накопители, диски, дискеты и т.п.) и неэлектронные (устройства ввода/вывода, важные записи и т.п.) носители информации;

каналы информационного обмена и телекоммуникации, в том числе коммуникационные протоколы;

системы и средства защиты информации;

объекты и помещения;

работники здравоохранения, являющиеся пользователями информационных ресурсов.

ГЛАВА 10
ВИДЫ И ИСТОЧНИКИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЗДРАВООХРАНЕНИИ

16. В основе угроз может лежать как природный, так и человеческий фактор.

16.1. Самым распространенным и опасным источником дестабилизирующего воздействия на защищаемую информацию являются нарушители. Это связано с тем, что воздействие на защищаемую информацию могут оказывать различные категории людей, как работающих, так и неработающих в здравоохранении в целом и в ОЗ в частности.

К этим источникам относятся:

сотрудники, работающие в здравоохранении, использующие средства автоматизации и информатизации и имеющие доступ к информационным ресурсам;

лица, не работающие в здравоохранении, но имеющие доступ к защищаемым активам в силу служебного положения;

лица, ведущие противоправную деятельность.

16.2. К источникам угроз, в основе которых лежит природный фактор, относятся угрозы, не зависящие от деятельности человека.

ГЛАВА 11
МОДЕЛЬ НАРУШИТЕЛЕЙ

17. В здравоохранении потенциальными нарушителями являются:

17.1. Внешние нарушители, которые могут пытаться со злонамеренными целями осуществить перехват данных, передаваемых по каналам связи, а также предпринимать технические атаки с целью получения доступа к защищаемой информации или нарушения безопасного функционирования ИС. Они могут обладать специальными знаниями об ИС, располагать как стандартным (доступным), так и специализированным оборудованием для идентификации уязвимости либо атаки, могут иметь высокую мотивацию осуществления атаки.

К внешним нарушителям относятся:

уволенные работники ОЗ;

представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности ОЗ (энергоснабжения, водоснабжения, теплоснабжения и т.п.);

пациенты;

лица, случайно или умышленно получившие доступ из внешних сетей к ИТ-инфраструктуре ОЗ (хакеры).

17.2. Внутренние нарушители, которые, в свою очередь, подразделяются на:

администраторов (системные администраторы МИС, администраторы сети и т.д.), которые могут допускать ошибки при управлении МИС и ИТ-инфраструктурой ОЗ в целом. Администраторы обладают специальными знаниями об инфраструктуре, как правило располагают специализированным оборудованием для идентификации уязвимости и атаки. Могут иметь мотивацию осуществления атаки, хотя являются доверенными привилегированными пользователями.

зарегистрированных пользователей (пользователи МИС), которые могут допускать ошибки при выполнении операций или пытаться получить нерегламентированный доступ к активам, например, из любопытства или иных незлонамеренных побуждений, в нарушение установленных для них прав доступа, воспользовавшись ошибками администрирования или недостатками в реализации системы. Зарегистрированные пользователи, как правило, не обладают специальными знаниями о МИС, располагают стандартным (доступным) оборудованием для идентификации уязвимости и атаки, могут получить мотивацию для злонамеренного осуществления атаки, хотя являются доверенными пользователями МИС;

внутренних нарушителей, не имеющих учетной записи в системе, но которые имеют к МИС какое-либо отношение. Действуют целенаправленно как из корыстных интересов или мести, так и из любопытства. Могут использовать весь набор методов и средств взлома СЗИ, пассивные средства (технические средства перехвата без

модификации компонентов системы), методы и средства активного воздействия (модификация программных и технических средств, подключение к каналам передачи данных, внедрение программных закладок и использование специальных инструментальных и технологических программ), а также комбинации воздействий как изнутри, так и извне – из сетей общего пользования. Такими нарушителями могут являться сотрудники, не допущенные к работе с МИС, технический персонал разного уровня (специалисты по обслуживанию технических средств, персонал, обслуживающий здание: уборщицы, электрики, сантехники), а также другие сотрудники, имеющие доступ в здание и помещения, где расположены СВТ.

ГЛАВА 12
МОДЕЛЬ УГРОЗ

18. Модель угроз представлена в виде описания вредоносного воздействия источников угроз, определенных в главе 9, и нарушителей, определенных в главе 10, на активы, определенные в главе 8 и подлежащие защите.

19. Общими угрозами защищаемым активам являются:

угрозы, связанные с физическим доступом к информационным ресурсам и системам;

нецелевое использование СВТ и сети Интернет;

утечка, в том числе по техническим каналам передачи данных, информации, распространение и (или) предоставление которой ограничено;

несанкционированный и (или) нерегламентированный доступ к защищаемым активам;

угрозы антропогенных и природных катастроф;

недостаточное обучение и неосведомленность работников ЦА Минздрава и ОЗ по вопросам обеспечения информационной безопасности;

юридические угрозы, связанные с:

нарушением (несоответствием требованиям) НПА и ЛНПА;

нарушением прав интеллектуальной собственности;

нелегальным использованием прикладного и системного ПО;

несанкционированным использованием информационных материалов, являющихся интеллектуальной собственностью;

нелегальным импортом/экспортом прикладного и системного ПО;

невыполнением договорных (контрактных) обязательств.

20. Кроме общих угроз защищаемым активам, существуют угрозы, направленные на нарушение основных свойств информации, которыми являются:

целостность, заключающаяся в существовании информации в неискаженном виде (неизменном по отношению к ее исходному состоянию);

конфиденциальность, заключающаяся в ограничении круга субъектов, имеющих доступ к информации;

доступность, заключающаяся в обеспечении своевременного и беспрепятственного доступа субъектов к интересующей их информации и готовности соответствующих автоматизированных служб к обслуживанию поступающих от субъектов запросов всегда, когда в этом возникает необходимость.

20.1. Угрозы конфиденциальности – это угрозы, которые позволяют нарушителю получить доступ к критичной информации. К нарушению конфиденциальности могут привести:

несанкционированные и (или) нерегламентированные действия легальных пользователей;

мониторинг сети, перехват и анализ сетевых сообщений;

имперсонификация, т.е. представление нарушителя как легального пользователя или устройства;

небрежное хранение резервных копий;

использование вредоносного ПО.

20.2. Угрозы целостности данных – это угрозы, которые могут разрушить целостность данных, хранящихся и обрабатываемых в ИС или передаваемых по техническим каналам связи в распределенных ИС. Под целостностью данных понимается гарантия того, что данные не могут быть изменены, модифицированы, разрушены или созданы злоумышленником.

К нарушениям целостности данных могут привести:

модификация, замена (вставка), удаление, перехват защищаемой информации;

фальсификация данных, передаваемых по каналам связи;

действие вредоносного ПО.

20.3. Угрозы доступности – это угрозы, которые не позволяют легальному пользователю получить доступ к интересующей его информации. Результатом реализации угроз может являть недоступность ИТ сервисов и разрушение (утрата) информационных ресурсов.

К нарушениям доступности защищаемых активов может привести атака «Отказ в обслуживании» (DoS, DDoS).

РАЗДЕЛ IV
ОСНОВНЫЕ ПОЛОЖЕНИЯ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ГЛАВА 13
ПОЛОЖЕНИЯ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

21. Требования по обеспечению ИБ обязательны к соблюдению всеми работниками здравоохранения и пользователями МИС.

22. Неисполнение или некачественное исполнение работниками здравоохранения и пользователями МИС обязанностей по обеспечению ИБ может повлечь лишение доступа к ИС, автоматизирующих деятельность ОЗ, а также применение к виновным мер, определенных законодательством и в НПА Минздрава.

23. Стратегия Минздрава в части противодействия угрозам ИБ заключается в сбалансированной реализации взаимодополняющих мер по обеспечению ИБ: от организационных мер на уровне Минздрава и ОЗ, до специализированных мер обеспечения ИБ по каждому выявленному в ОЗ инциденту ИБ, основанных на оценке рисков ИБ.

24. С целью поддержки заданного уровня защищенности руководство Минздрава придерживается процессного подхода в построении СУИБ. СУИБ здравоохранения основывается на осуществлении следующих основных процессов: планирование, реализация и эксплуатация защитных мер, проверка (мониторинг и анализ) и совершенствование, соответствующих положениям национальных и международных стандартов по обеспечению ИБ. Реализация этих процессов осуществляется в виде непрерывного, направленного на постоянное совершенствование деятельности по обеспечению ИБ здравоохранения и повышение ее эффективности.

25. На всех этапах жизненного цикла управление ИБ здравоохранения осуществляется с соблюдением НПА, определяющих процессы управления ИБ здравоохранения.

ГЛАВА 14
ПЛАНИРОВАНИЕ МЕРОПРИЯТИЙ ПО ОБЕСПЕЧЕНИЮ ИБ ЗДРАВООХРАНЕНИЯ

26. При планировании мероприятий по обеспечению ИБ здравоохранения осуществляются:

26.1. определение и распределение ролей, связанных с обеспечением ИБ (ролей ИБ);

26.2. оценка важности информационных активов с учетом потребности в обеспечении их свойств с точки зрения ИБ;

26.3. управление рисками ИБ, включающие:

анализ влияния на ИБ применяемых в деятельности ОЗ технологий, а также внешних по отношению к ОЗ событий;

выявление проблем обеспечения ИБ, анализ причин их возникновения и прогнозирование их развития;

определение моделей угроз ИБ;

выявление, анализ и оценка значимых угроз ИБ;

выявление возможных негативных последствий для ОЗ, наступающих в результате проявления факторов риска ИБ, в том числе связанных с нарушением свойств безопасности информационных активов ОЗ;

идентификацию и анализ рисковых событий ИБ;

оценку величины рисков ИБ и определение среди них рисков, неприемлемых для ОЗ;

обработку результатов оценки рисков ИБ, базирующейся на методах управления, определенных положениям национальных и международных стандартов по управлению рисками ИБ, а также НПА Минздрава;

оптимизацию рисков ИБ за счет выбора и применения защитных мер, противодействующих проявлениям факторов риска и минимизирующих возможные негативные последствия для ОЗ в случае наступления рисковых событий;

оценку влияния защитных мер на цели основной деятельности здравоохранения;

оценку затрат на реализацию защитных мер;

рассмотрение и оценку различных вариантов решения задач по обеспечению ИБ;

разработку планов управления рисками, предусматривающих различные защитные меры и варианты их применения, и выбор из них такого, реализация которого максимально положительно скажется на целях основной деятельности здравоохранения и будет оптимальна с точки зрения произведенных затрат и ожидаемого эффекта;

документальное оформление целей и задач обеспечения ИБ здравоохранения, поддержка в актуальном состоянии нормативно–методического обеспечения деятельности в сфере ИБ.

ГЛАВА 15
ДЕЯТЕЛЬНОСТЬ ПО ОБЕСПЕЧЕНИЮ ИБ

27. В рамках реализации деятельности по обеспечению ИБ здравоохранения осуществляются:

27.1. менеджмент инцидентов ИБ, включающий:

сбор информации о событиях ИБ;

выявление и анализ инцидентов ИБ;

расследование инцидентов ИБ;

оперативное реагирование на инцидент ИБ;

минимизация негативных последствий инцидентов ИБ;

оперативное доведение до руководства Минздрава информации по наиболее значимым инцидентам ИБ и оперативное принятие решений по ним, включая регламентирование порядка реагирования на инциденты ИБ;

выполнение принятых решений по всем инцидентам ИБ в установленные сроки;

пересмотр применяемых требований, мер и механизмов по обеспечению ИБ по результатам рассмотрения инцидентов ИБ;

повышение уровня знаний работников здравоохранения в вопросах обеспечения ИБ;

обеспечение регламентации и управления доступом к программным и программно-техническим средствам и сервисам ИС здравоохранения и информации, обрабатываемой в них;

применение средств криптографической защиты информации;

обеспечение бесперебойной работы ИС и сетей связи;

обеспечение возобновления работы ИС и сетей связи после прерываний и нештатных ситуаций;

применение средств защиты от вредоносного ПО;

обеспечение ИБ на стадиях жизненного цикла ИС здравоохранения, связанных с проектированием, разработкой, приобретением, поставкой, вводом в действие, сопровождением (сервисным обслуживанием);

обеспечение ИБ при использовании доступа в сеть Интернет и услуг электронной почты;

контроль доступа в здания и помещения.

27.2. обеспечение защиты информации от утечки по техническим каналам, включающее:

применение мер и технических средств, снижающих вероятность несанкционированного получения информации в устной форме – пассивная защита;

применение мер и технических средств, создающих помехи при несанкционированном получении информации – активная защита;

применение мер и технических средств, позволяющих выявлять каналы несанкционированного получения информации – поиск.

ГЛАВА 16
ПРОВЕРКА ДЕЯТЕЛЬНОСТИ ПО ОБЕСПЕЧЕНИЮ ИБ

28. В целях проверки деятельности по обеспечению ИБ здравоохранения осуществляются:

контроль правильности реализации и эксплуатации защитных мер;

контроль изменений конфигурации ИС здравоохранения;

мониторинг факторов рисков и соответствующий их пересмотр;

контроль реализации и исполнения требований работниками здравоохранения действующих НПА и ЛНПА по обеспечению ИБ отрасли;

контроль деятельности пользователей ИС здравоохранения, направленный на выявление и предотвращение конфликтов интересов.

ГЛАВА 17
СОВЕРШЕНСТВОВАНИЕ ДЕЯТЕЛЬНОСТИ ПО ОБЕСПЕЧЕНИЮ ИБ

29. В целях совершенствования деятельности по обеспечению ИБ здравоохранения осуществляется периодическое, а при необходимости оперативное, уточнение/пересмотр целей и задач обеспечения ИБ.

РАЗДЕЛ V
РОЛИ И СФЕРЫ ОТВЕТСТВЕННОСТИ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ГЛАВА 18
РОЛИ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

30. В целях выполнения задач по обеспечению ИБ здравоохранения, в соответствии с рекомендациями международных и национальных стандартов по ИБ в отрасли должны быть определены следующие роли ИБ:

Министр здравоохранения Республики Беларусь;

Куратор ИБ;

ответственное подразделение ИБ здравоохранения;

должностное лицо, ответственное за ИБ в главных управлениях по здравоохранению облисполкомов, комитете по здравоохранению Минского горисполкома и в ОЗ (подразделение по обеспечению ИБ ОЗ);

работники здравоохранения.

31. При необходимости могут быть определены и другие роли ИБ.

32. К сфере ответственности Министра здравоохранения Республики Беларусь относится определение Политики ИБ отрасли.

33. Куратор ИБ назначается из числа заместителей Министра здравоохранения Республики Беларусь.

34. Куратором ИБ не может являться заместитель Министра здравоохранения Республики Беларусь, курирующий вопросы внедрения и развития ИТ в здравоохранении.

35. К сфере ответственности Куратора ИБ относится:

координация и организация внедрения мер по обеспечению ИБ здравоохранения.

обеспечение назначения, определение обязанностей и полномочий в отношении соответствующих ролей, имеющих отношение к ИБ;

согласование назначения должностных лиц, ответственных за ИБ в ГО.

36. Ответственное подразделение ИБ здравоохранения осуществляет деятельность и планирование деятельности по обеспечению ИБ в здравоохранении.

37. К сфере ответственности ответственного подразделения относятся:

установление потребностей ОЗ в применении мер обеспечения ИБ, определяемых НПА и ЛНПА Минздрава;

контроль соблюдения национального законодательства, нормативных актов органов государственного регулирования в области обеспечения защиты информации, НПА, ЛНПА Минздрава и национальных стандартов по обеспечению ИБ в ОЗ;

разработка и поддержание в актуальном состоянии нормативных документов по обеспечению ИБ здравоохранения, включая Концепцию ИБ, планы, политики, положения, регламенты, инструкции, методики, перечни сведений и иные виды нормативных документов Минздрава;

осуществление контроля актуальности и непротиворечивости НПА Минздрава и ОЗ (политик, положений, планов, методик и т.д.), затрагивающих вопросы обеспечения ИБ ОЗ;

обучение, контроль и непосредственная работа с работниками отрасли в области обеспечения ИБ;

выявление и предотвращение реализации угроз ИБ;

выявление инцидентов ИБ и реагирование на них;

учет инцидентов ИБ, выявленных в ОЗ;

информирование в установленном порядке ОАЦ и правоохранительных органов об угрозах и событиях ИБ;

прогнозирование и предупреждение инцидентов ИБ;

пресечение несанкционированных действий нарушителей ИБ;

формирование и поддержание в актуальном состоянии базы инцидентов ИБ, анализ, разработка оптимальных процедур реагирования на инциденты;

типизация решений по применению мер и средств обеспечения ИБ и распространение типовых решений на ОЗ;

мониторинг и оценка ИБ отрасли, включая оценку полноты и достаточности защитных мер и видов деятельности по обеспечению ИБ в ОЗ и отрасли в целом;

контроль обеспечения ИБ в отрасли, в том числе, и на основе информации об инцидентах ИБ, результатах мониторинга, оценки и аудита ИБ;

информирование руководства Минздрава и руководителей ОЗ об угрозах ИБ, влияющих на деятельность ОЗ;

взаимодействие с ОАЦ по вопросам обеспечения ИБ отрасли.

38. Ответственное подразделение ИБ здравоохранения может создавать оперативные группы для проведения расследований инцидентов ИБ, возглавляемые работником ответственного подразделения, и, при наличии обоснованной необходимости, по согласованию с куратором, привлекать для работы специализированные организации, имеющие специальное разрешение (лицензию) ОАЦ на соответствующие виды работ по технической и криптографической защите информации.

39. Финансирование работ по реализации положений Концепции ИБ осуществляется в рамках выделенных финансовых средств.

40. Должностными лицами, ответственными за ИБ в главных управлениях по здравоохранению облисполкомов, комитете по здравоохранению Минского горисполкома и в ОЗ, назначаются должностные лица уровня заместителя руководителя.

41. Должностными лицами, ответственными за ИБ, не могут являться заместители руководителей, курирующие вопросы внедрения, эксплуатации и развития ИТ в подчиненных ОЗ.

42. Основными задачами должностных лиц, ответственных за ИБ, при выполнении возложенных на них обязанностей и в рамках их участия в деятельности ОЗ по обеспечению ИБ являются:

разработка и поддержание в актуальном состоянии ЛНПА, определяющих политику ИБ, а также основные вопросы обеспечения ИБ в

главных управлениях здравоохранения областных исполнительных комитетов, комитета по здравоохранения Минского городского исполнительного комитета и ОЗ;

контроль соблюдения требований ИБ, устанавливаемых НПА и ЛНПА;

выявление и предотвращение реализации угроз ИБ в пределах своей компетенции;

выявление и реагирование на инциденты ИБ;

информирование в установленном порядке ответственное подразделение ИБ здравоохранения о выявленных угрозах и событиях ИБ;

прогнозирование и предупреждение инцидентов ИБ в ОЗ;

мониторинг и оценка ИБ в рамках своего участка работы (ОЗ, главное управление по здравоохранению, комитет по здравоохранению Минского горисполкома);

информирование руководства ОЗ, главного управления по здравоохранению, комитета по здравоохранению Минского горисполкома (по принадлежности) и ответственного подразделения ИБ здравоохранения о выявленных угрозах в информационной среде ОЗ.

43. Для обеспечения реализации требований ИБ, устанавливаемых НПА и ЛНПА, в ОЗ республиканского подчинения, а также в ОЗ, имеющих территориально распределенную структуру, может быть создано подразделение по обеспечению ИБ.

44. Основными задачами подразделения по обеспечению ИБ ОЗ являются:

разработка и поддержание в актуальном состоянии ЛНПА, определяющих политику ИБ, а также основные вопросы обеспечения ИБ в ОЗ;

контроль соблюдения требований ИБ, устанавливаемых НПА и ЛНПА;

выявление и предотвращение реализации угроз ИБ в пределах своей компетенции;

выявление и реагирование на инциденты ИБ;

информирование в установленном порядке ответственное подразделение ИБ здравоохранения о выявленных угрозах и событиях ИБ;

прогнозирование и предупреждение инцидентов ИБ в ОЗ;

мониторинг и оценка ИБ ОЗ;

информирование руководства ОЗ, главного управления здравоохранения облисполкома, комитета по здравоохранению Минского горисполкома (по принадлежности), а также ответственного подразделения ИБ здравоохранения о выявленных угрозах в информационной среде ОЗ.

45. Основными задачами работников отрасли по обеспечению ИБ при выполнении возложенных на них обязанностей являются:

соблюдение требований ИБ, устанавливаемых НПА и ЛНПА;

выявление и предотвращение реализации угроз ИБ в пределах своей компетенции;

выявление инцидентов ИБ и информирование о них уполномоченных должностных лиц;

информирование в установленном порядке должностных лиц, ответственных за ИБ, и руководство ОЗ о выявленных угрозах, в том числе и в информационной среде ОЗ.

РАЗДЕЛ VI
ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

ГЛАВА 19
ОТВЕТСТВЕННОСТЬ ЗА СОБЛЮДЕНИЕ ПОЛОЖЕНИЙ КОНЦЕПЦИИ ИБ

46. Общее руководство обеспечением ИБ здравоохранения осуществляет Куратор ИБ.

47. Ответственность за поддержание положений настоящей Концепции ИБ в актуальном состоянии, создание, внедрение, координацию и внесение изменений в процессы СУИБ здравоохранения лежит на руководстве ответственного подразделения ИБ здравоохранения.

48. Ответственность работников здравоохранения за невыполнение настоящей Концепции ИБ определяется соответствующими положениями, включаемыми в должностные инструкции работников, а также законодательством.

ГЛАВА 20
ПОРЯДОК ПЕРЕСМОТРА КОНЦЕПЦИИ ИБ

49. Концепция ИБ подлежит пересмотру (актуализации) не реже одного раза в три года.

50. Внесение изменений в Концепцию ИБ осуществляется на периодической и внеплановой основе:

периодическое внесение изменений должно осуществляться не реже одного раза в 36 месяцев;

внеплановое внесение изменений может производиться по результатам анализа инцидентов ИБ, актуальности, достаточности,

эффективности используемых мер обеспечения ИБ, по результатам проведения аудитов ИБ и других контрольных мероприятий.

51. В случае изменения законодательства и иных нормативных актов, Концепция ИБ и изменения к ней применяются в части, не противоречащей вновь принятым законодательным и иным нормативным актам. В этом случае Ответственное подразделение ИБ здравоохранения обязано незамедлительно инициировать внесение соответствующих изменений.

52. Ответственным за внесение изменений в настоящую Концепцию является руководитель ответственного подразделения ИБ здравоохранения.

53. Пересмотр и актуализация Концепции ИБ осуществляется ответственным подразделением ИБ здравоохранения и утверждается приказом Министра здравоохранения Республики Беларусь.

ГЛАВА 21
КОНТРОЛЬ СОБЛЮДЕНИЯ ПОЛОЖЕНИЙ КОНЦЕПЦИИ ИБ

54. Общий контроль состояния ИБ осуществляется Куратором ИБ.

55. Текущий контроль соблюдения Концепции ИБ осуществляет ответственное подразделение ИБ здравоохранения. Контроль осуществляется путем проведения мониторинга и менеджмента инцидентов ИБ, по результатам оценки ИБ, а также в рамках иных контрольных мероприятий.

56. Ответственное подразделение ИБ здравоохранения осуществляет контроль соблюдения Концепции ИБ в ОЗ на основе проведения аудита ИБ ОЗ.