УТВЕРЖДЕНО
Приказ директора
РНПЦ детской хирургии
26.08.2024 № 159

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВЕННОГО УЧРЕЖДЕНИЯ «РЕСПУБЛИКАНСКИЙ НАУЧНО-ПРАКТИЧЕСКИЙ ЦЕНТР ДЕТСКОЙ ХИРУРГИИ»

г. Минск 2024

СОДЕРЖАНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Политика информационной безопасности (далее – Политика ИБ) государственного учреждения «Республиканский научно-практический центр детской хирургии» (далее – Центр) разработана в соответствии с требованиями Положения о порядке технической и криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, утвержденного приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г.№ 66 «О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449».

1.2. В соответствии с требованиями законодательствам Республики Беларусь в сфере защиты информации, информация, распространение и (или) предоставление которой ограничено, а также информация, содержащаяся в государственных информационных системах, должна обрабатываться в информационных системах с применением системы защиты информации. Эксплуатация информационных систем без реализации мер по защите информации не допускается.

1.3. Политика ИБ является основополагающим документом Центра в области информационной безопасности и устанавливает документально закрепленные общие намерения по обеспечению конфиденциальности, целостности, сохранности, подлинности и доступности информации, которые детализируются (регламентируются) посредством частных Политик, перечень которых приведен в Приложении 1.

1.4. Обеспечение рациональности и результативности Политики ИБ является основой эффективности функционирования системы защиты информации информационной системы Центра.

1.5. Лицом, ответственным за организацию информационной безопасности в Центре, является заместитель директора по безопасности, режиму и кадрам.

1.6. Лицами, ответственными за защиту информации в Центре, являются:

в целом по Центру – специалист по защите информации;

в структурных подразделениях – их непосредственные руководители.

2. ОСНОВНЫЕ ТЕРМИНЫ, ИХ ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ

2.1. В настоящей Политике ИБ применяются термины и их обозначения установленные:

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

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

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

приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 20.02.2020 № 66 «О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449».

2.2 В Политике ИБ применяются следующие термины и их определения:

вредоносное программное обеспечение – программный код (исполняемый или интерпретируемый), обладающий свойством несанкционированного воздействия на объект информационной системы;

доступность – свойство информации быть доступной и используемой по запросу со стороны уполномоченного пользователя;

информационная безопасность – состояние информационной системы, при котором с требуемой вероятностью обеспечиваются конфиденциальность, целостность, подлинность, доступность и сохранность защищаемой информации;

информационная система (далее – ИС) – совокупность банков данных, информационных технологий и комплекса (комплексов) программно-технических средств;

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

конфиденциальность – свойство информации, заключающееся в недоступности информации или не раскрытии ее содержания для неавторизованных лиц, процессов и логических объектов;

машинный носитель информации (далее – МНИ) – любое техническое устройство, используемое средством вычислительной техники для фиксации, хранения, накопления, преобразования и передачи информации;

объект информационной системы – пассивная сущность в пределах информационной системы, которая содержит или получает информацию и над которой субъекты выполняют операции;

отказ – событие, состоящее из нарушения работоспособности средств вычислительной техники, средств технической защиты информации и иных технических средств из состава информационной системы, для восстановления которой требуется замена составной части или ее регулировка (настройка);

отчуждаемый (съемный) МНИ – МНИ способный подключаться к СВТ без вмешательства в системный блок;

пароль – набор знаков, предназначенный для подтверждения личности и (или) полномочий;

подлинность – свойство информации, гарантирующее, что информация идентична оригинальной (заявленной);

пользователь информационной системы – лицо или внешний объект информационных технологий, взаимодействующий с ИС;

программное обеспечение (далее – ПО) – набор команд, управляющих работой средств вычислительной техники;

система защиты информации (далее – СЗИ) – комплекс правовых, организационных и технических мер, направленных на обеспечение конфиденциальности, целостности, подлинности, доступности и сохранности информации;

сохранность – свойство информации, гарантирующее, что информация ни при каких условиях не может быть уничтожена (удалена);

средство вычислительной техники (далее – СВТ) – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем;

средство технической защиты информации (далее – СТЗИ) – технические, программные, программно-аппаратные средства защиты информации, предназначенные для защиты информации от ее утечки по техническим каналам, несанкционированного доступа, несанкционированных воздействий на информацию, блокирования правомерного доступа к ней, иных неправомерных воздействий на информацию, а также для контроля эффективности ее защищенности;

техническая защита информации (далее – ТЗИ) – деятельность, направленная на обеспечение конфиденциальности, целостности, доступности и сохранности информации техническими мерами без применения средств криптографической защиты информации;

угроза информационной безопасности – совокупность условий и факторов, создающих опасность нарушения информационной безопасности;

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

2.3 В настоящей Политике ИБ применяются следующие сокращения:

НПА – нормативные правовые акты Республики Беларусь;

ОС – операционная система;

ППО – прикладное программное обеспечение;

ТНПА – технические нормативные правовые акты.

ЭЦП – электронная цифровая подпись.

3. ОБЩИЕ СВЕДЕНИЯ

3.1 Политика ИБ – это официально сформулированные Центром общие намерения и направления деятельности по обеспечению конфиденциальности, целостности, подлинности, доступности и сохранности информации при ее обработке в ИС.

3.2 Политика ИБ определяет базовые решения по организации СЗИ ИС и по построению устойчивой, надежной, безопасной технологии обработки защищаемой информации, в том числе:

цели и принципы защиты информации в Центре;

перечень ИС, отнесенных к соответствующим классам типовых ИС, а также отдельно стоящих персональных электронных вычислительных машин (далее – ПЭВМ), используемых в Центре и принадлежащих ей на праве собственности или ином законном основании;

обязанности пользователей ИС;

порядок взаимодействия с иными ИС.

3.3 Политика ИБ служит основой для проведения работ по созданию СЗИ ИС и определяет пути ее совершенствования, а также является руководством по регламентации действий работников Центра по рассматриваемому направлению деятельности.

3.4 Политика ИБ документируется с учетом требований нормативных правовых актов Республики Беларусь, регламентирующих деятельность по технической и криптографической защите информации.

3.5 Политика ИБ представляется для использования работниками Центра, осуществляющими функциональное использование, техническое и программное сопровождение ИС и, при необходимости, работникам сторонних организаций, оказывающих услуги (выполняющим работы) для Центра.

3.6 Обеспечение постоянной пригодности, адекватности и результативности Политики ИБ является основой эффективности функционирования СЗИ ИС.

3.7 Директор, его заместители, руководители структурных подразделений (далее – Руководство) Центра, а также специалист по защите информации, проводят систематический мониторинг реализации требований Политики ИБ с целью обеспечения ее актуальности и эффективности.

3.8 Реализация Политики ИБ должна осуществляться на основе принципов непрерывности и строгого соблюдения установленных правил.

3.9 Действие настоящей Политики ИБ подлежит пересмотру и корректировке в том случае, если происходят существенные изменения в гарантии ее непрерывного соответствия установленным требованиям и эффективности применения, в том числе при изменении организационной или технологической инфраструктуры ИС, условий ее эксплуатации; а также при изменении законодательства Республики Беларусь в рассматриваемой сфере деятельности.

3.10 Нарушение требований Политики ИБ влечет ответственность в соответствии с законодательством Республики Беларусь

4. ЦЕЛИ, ЗАДАЧИ И ПРИНЦИПЫ ПОСТРОЕНИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

4.1. СЗИ Центра включает комплекс мер, направленных на обеспечение конфиденциальности, целостности, подлинности, доступности и сохранности информации в ИС.

4.2. Объектами СЗИ ИС Центра (далее – Активы) являются:

ИС (ресурсы);

данные, обрабатываемые и формируемые в результате выполнения автоматизированных процессов в ИС;

данные, используемые для управления оборудованием ИС и режимами ее функционирования, реализации настроек безопасности, контроля над событиями безопасности;

каналы информационного обмена;

оборудование ИС (ПЭВМ, автоматизированные рабочие места, периферийное оборудование, средства телекоммуникаций, средства защиты информации), предоставляемые пользователям и (или) процессам обработки информации;

ПО (общесистемное, прикладное), обеспечивающее реализацию автоматизированных процессов деятельности организации на базе предоставляемых ресурсов ИС;

документация, регламентирующая содержание и порядок функционирования СЗИ ИС Центра.

4.3 СЗИ Активов строится на принципах:

соблюдения Конституции Республики Беларусь, законодательства Республики Беларусь, локальных правовых актов и методических рекомендации (материалов) Центра (далее – ЛПА);

правового равенства всех участников процесса информационного взаимодействия при условии осуществления поиска, получения и распространения информации любым законным способом;

рассмотрения информационных ресурсов в качестве объектов собственности;

соответствия ограничения доступа, устанавливаемого действующим законодательством Республики Беларусь и ЛПА, направленных на обеспечение ИБ Центра;

невозможности обхода СЗИ, в соответствии с которым все информационные потоки внутри Активов, а также при взаимодействии Активов с внешними системами и пользователями, должны контролироваться;

невозможности перехода защитных средств в небезопасное состояние, т.е. при любых обстоятельствах, в том числе нештатных, они либо полностью выполняют свои функции, либо полностью блокируют доступ к Активам;

достижения своевременности, эффективности (адекватности, пропорциональности), интеграции, согласованности и непрерывности защитных мер реальным угрозам и рискам ИБ, направленных на:

предупреждение условий, порождающих угроз Активам;

обнаружение проявившихся угроз ИБ;

обнаружение воздействия угроз на Активы;

локализацию и ликвидацию воздействия угроз на Активы;

разделения полномочий (обязанностей) – разделение ролей и ответственности, при котором ни один человек не имеет полномочий, позволяющих ему единолично осуществлять выполнение критических операций, и не может нарушать критически важный для организации процесс или создать уязвимость в защите по заказу злоумышленников, сговора между сотрудниками или для предотвращения злонамеренных, неквалифицированных действий;

усиления самого слабого звена, выявленного при регулярном обследовании защищаемых Активов;

постоянного совершенствования СЗИ за счет периодической переоценки защитных мер и потребности в них, поддержания Политики ИБ и ЛПА в актуальном состоянии, назначении интервалов их пересмотра и корректировки;

запрещено все, что явно не разрешено;

персональной ответственности при совершении неправомерных действий.

4.3. Основными целями СЗИ Активов являются:

регламентирование подходов к обеспечению защиты информационных ресурсов в Центре;

сохранение и неразглашение информации о частной жизни физических лиц и неразглашение персональных данных, служебной информации ограниченного распространения, информации, составляющей врачебную и иную охраняемую законом тайну, содержащихся в ИС и отдельно стоящих ПЭВМ (АРМ);

обеспечение прав субъектов информационных отношений при создании, использовании и эксплуатации ИС;

недопущение неправомерного доступа, уничтожения, модификации (изменения), копирования, распространения и (или) предоставления информации, блокирования правомерного доступа к персональным данным, врачебной тайне, содержащихся в ИС (ресурсах), а также иных неправомерных действий;

минимизация ущерба от реализации угроз ИБ в отношении ИС;

осуществление контроля за соблюдением требований ИБ и порядком использования Активов, определенных в ЛПА.

4.4 Достижение основных целей СЗИ Активов обеспечивается решением следующих задач:

своевременное выявление и прогнозирование источников угроз Активам;

оценка возможного воздействия угроз на Активы и потенциальных последствий такого воздействия;

оперативное реагирование на угрозы безопасности информации путем принятия своевременных мер по недопущению нарушения ИБ Активов и (или) снижению негативных последствий нарушения безопасности;

назначение работникам Центра, а также работникам сторонних организаций прав доступа и полномочий по доступу к Активам только в том объеме, который необходим им для выполнения своих должностных обязанностей, предусмотренных условиями должностных инструкций или работ, в соответствии с договором;

предоставление доступа к Активам только авторизованным пользователям после их успешной идентификации и аутентификации, предотвращение и блокирование попыток неавторизованного доступа к Активам;

ограничение физического доступа посторонних лиц к средствам обработки и хранения информации;

недопущение передачи служебной информации ограниченного распространения, персональных данных и информации, составляющей врачебную тайну, по общедоступным каналам электросвязи без применения средств криптографической защиты информации;

контроль обеспечения ИБ Активов при использовании услуг по разработке, модернизации, внедрению, обслуживанию, сопровождению, резервированию и администрированию ИС или их компонентов, оказываемых сторонними организациями;

заблаговременное принятие эффективных мер по восстановлению безопасного состояния Активов на случай возможного нарушения ИБ в результате реализации угроз;

надлежащее применение криптографических средств защиты информации в соответствии с законодательством;

контроль состояния защищенности и эффективное управление ИБ Активов;

формирование структурированной системы учета Активов и иных объектов СЗИ ИС (ПЭВМ, ПО, ЭЦП и т.п) в интересах обеспечения оперативности при возникновении необходимости принятия управленческих решений и определения персональной ответственности при нарушениях требований законодательства Республики Беларусь и ЛПА в сфере ИБ.

5. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ СИСТЕМ И ПЕРЕЧЕНЬ СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

5.1. В Центре используется:

информационная система «РНПЦ детской хирургии», отнесенная к классу типовых информационных систем «3-спец», «3-ин», «3-юл»;

информационная система «Мобильное автоматизированное рабочее место, предназначенное для обработки документов, содержащих служебную информацию ограниченного распространения», отнесенная к классу типовых информационных систем «4-дсп».

5.2. Перечень ПЭВМ, используемых в ИС (далее – Перечень), ведется работником отдела автоматизированных систем управления (далее – АСУ), определяемым решением начальника отдела АСУ.

Допускается ведение Перечня в электронном виде.

5.3. Перечень должен включать в себя следующие сведения о средстве вычислительной техники:

номер по порядку;

наименование (модель) и инвентарных номер ПЭВМ (при наличии);

место нахождения (номер кабинета);

и другую необходимую информацию.

5.4. Для обработки информации ограниченного распространения и имеющей гриф «Для служебного пользования» в Центре необходимо использовать отдельную ИС имеющую установленный законодательством Республики Беларусь аттестат соответствия системы защиты информации требованиям по защите информации.

6. ОСНОВНЫЕ ПОЛОЖЕНИЯ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ

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

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

соблюдение законодательства Республики Беларусь в области защиты информации;

разработка и распределение в установленном порядке должностных обязанностей работников Центра, участвующих в обеспечении ИБ;

внесение изменений и дополнений в трудовые договоры и организационно-распорядительные документы (положения о структурных подразделениях, должностные инструкции и т.п) по вопросам обеспечения ИБ;

подготовка приказов, распоряжений, методических материалов, касающихся вопросов защиты информации;

подготовка документов по вопросам регламентации отношений

между Центром и сторонними организациями, предоставляющими услуги, в части обеспечения безопасности Активов;

определение в договорах (соглашениях) на обслуживание (техническое сопровождение ПО и др.) со сторонними организациями, ответственности в отношении конфиденциальной информации (информации ограниченного распространения), доступ к которой может быть получен в ходе выполнения договорных обязательств, а также ответственность сторон по договору за нарушение указанных условий.

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

6.4. К основным организационным мерам относятся:

проведение учета и категорирования Активов с назначением владельцев Активов, поддержание учетных данных в актуальном состоянии;

выявление наиболее вероятных потенциальных угроз для Активов, выявление уязвимых мест процессов обработки, передачи и хранения информации в обеспечении ИБ Активов;

оценка возможного ущерба деятельности Центра, вызванного нарушением ИБ Активов;

оценка рисков ИБ и определение организационных и технических мер по защите информации с целью недопущения неприемлемых рисков ИБ;

определение порядка предоставления (изменения, прекращения) работникам Центра и работникам сторонних организаций необходимых полномочий по доступу к Активам;

разработка правил управления доступом к Активам, режимов обработки данных и доступа к ним;

определение порядка и правил учета и категорирования Активов;

определение перечня необходимых мер по обеспечению штатного функционирования ИС и ее компонентов в критических ситуациях, возникающих в результате несанкционированного доступа к Активам, сбоев и отказов технических средств, ошибок программного обеспечения и пользователей, стихийных бедствий и т.п.;

определение порядка и правил резервного копирования и восстановления информации;

определение порядка и правил антивирусной защиты Активов;

определение порядка доступа работников Центра к внешним сетям, в том числе к глобальной компьютерной сети Интернет (далее – Интернет), а также правил надлежащего использования общедоступных сервисов;

определение порядка учета, выдачи, использования и хранения машинных носителей информации, используемых для создания и хранения резервных (архивных) копий информации, а также информационного обмена (при необходимости);

установление правил обеспечения безопасности при использовании работниками мобильных средств обработки и хранения данных, удаленном доступе к Активам с использованием таких средств;

определение категорий лиц, имеющих доступ в помещения, в которых установлены серверное и коммуникационное оборудование, технические средства обработки и защиты информации ИС;

организация делопроизводства (разработка, учет, хранение, отправка, использование, уничтожение носителей информации и др.) со служебной информацией ограниченного распространения;

контроль за соблюдением работниками Центра и сторонними организациями, оказывающими услуги или пользующихся информационными услугами Центра, требований и правил по обеспечению ИБ Активов, установленных настоящей Политикой и ЛПА;

контроль за формированием и реализацией требований ИБ при модернизации (обновлении) программного и аппаратного обеспечения ИС или ее отдельных компонентов;

периодический анализ состояния и оценка эффективности применяемых мер по ЗИ;

определение и реализация мер сетевой безопасности Активов;

поддержание в актуальном состоянии проектной и эксплуатационной документации на ИС и ее компоненты с отражением в ней аспектов, связанных с обеспечением ИБ;

обучение (инструктаж, информирование) работников Центра и сторонних организаций по выполнению требований ИБ при работе с Активами;

разграничение доступа к информации по кругу лиц и характеру информации.

6.5. К основным техническим мерам по защите информации в ИС относятся:

настройка доступа в ИС только авторизованных пользователей после прохождения успешной идентификации и аутентификации;

систематическое резервное копирование данных и информации;

применение сертифицированных средств защиты и лицензионного программного обеспечения;

применение средств криптографической защиты информации для защиты конфиденциальности, целостности и подлинности информации при ее передаче по каналам связи общего доступа;

контроль функционирования и управление применяемыми в ИС СЗИ;

регистрация событий безопасности, связанных с действиями пользователей при работе с Активами и управлением режимами функционирования компонентов ИС и СЗИ;

своевременное обнаружение нарушений ИБ и принятие соответствующих мер по восстановлению безопасного состояния ИС;

ликвидация (снижение) последствий (локализация) нарушения ИБ;

применение следующих мер обеспечения защиты Активов от угроз при взаимодействии с сетью Интернет и сторонними ИС:

фильтрация сетевых пакетов в соответствии с задаваемыми правилами на основе IP-адресов отправителя и получателя, разрешенных портов, протоколов и приложений;

управление сетевым доступом к ИС;

обнаружение атак с использованием известных шаблонов атак;

обновление базы сигнатур обнаружения вторжений;

антивирусная фильтрация трафика, получаемого из глобальной компьютерной сети Интернет, и антивирусная защита Активов;

регистрация событий ИБ с заданным уровнем детализации;

обеспечение отказоустойчивости аппаратных (виртуальных) средств защиты информации.

7. ОБЯЗАННОСТИ СУБЪЕКТОВ ИНФОРМАЦИОННЫХ ОТНОШЕНИЙ

7.1. Субъектами информационных отношений в Центре являются:

Центр, как владелец (оператор) информационных систем (ресурсов) и их компонентов;

юридические лица, являющиеся разработчиками информационных ресурсов (систем) используемых Центром, и выступающие в качестве их операторов.

7.2. Должностные лица субъектов информационных отношений:

руководство Центра, в соответствии с обязанностями, возложенными на них должностными инструкциями;

работники отдела АСУ, участвующие в обеспечении безопасного функционирования информационных систем (ресурсов), их компонентов и инфраструктуры (далее – администраторы системы);

специалист по защите информации (в период его временного отсутствия – лицо, исполняющее его обязанности на основании приказа директора Центра, в рамках исполнения которых получившие доступ к СЗИ ИС);

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

7.3. Директор центра несет персональную ответственность за организацию работ по технической и криптографической защите информации.

7.4. Заместитель директора по безопасности, режиму и кадрам:

координирует организацию и планирование мероприятий ИБ в Центре;

осуществляет общий контроль всего комплекса мероприятий по обеспечению ИБ в Центре;

обеспечивает соблюдение требований законодательства в области ИБ и взаимодействие ответственных работников Центра с регулирующими органами (поставщиками) телекоммуникационных услуг по вопросам, связанными с ИБ.

7.5. Руководители структурных подразделений Центра принимают меры по обеспечению сохранности информации, распространение и (или) предоставление которой ограничено, в подчиненных подразделениях и в пределах своей компетенции осуществляют контроль за соблюдением подчиненными работниками требований настоящей Политики и ЛПА по обеспечению ИБ в Центре.

7.6. Специалист по защите информации осуществляет планирование, сопровождение, координацию и контроль работ по обеспечению ИБ в Центре, а также выполняет следующие функции.

7.6.1 Лично:

обеспечение соблюдения в Центре требований законодательства и ЛПА в области ИБ;

обеспечение функционирования и развитие СЗИ Активов;

определение требований по защите информации в процессе разработки, внедрения, обеспечения функционирования и развития Активов;

определение комплекса мер по технической и криптографической защите обрабатываемой в Активах информации, распространение и (или) предоставление которой ограничено, не содержащей сведения, отнесенные к государственным секретам;

пресечение действий нарушителей ИБ;

разработка, внедрение и поддержание в актуальном состоянии настоящей Политики и организационно-распорядительной документации, регламентирующей вопросы обеспечения ИБ в Центре;

учет и категорирование Активов;

разработка (корректировка) технического задания на СЗИ, создание и проведение испытаний (аттестации, переаттестации) СЗИ Активов;

контроль соблюдения работниками Центра и сторонних организаций требований по защите информации, установленных настоящей Политикой и ЛПА, анализ (обобщение) результатов контроля и их доведение до руководства Центра(в части касающейся);

взаимодействие с работниками Центра по вопросам обеспечения ИБ (информирование, обучение, консультирование);

информирование Руководства Центра (владельцев Актива) об угрозах и инцидентах ИБ, влияющих на деятельность центра;

взаимодействие с регулирующими органами и поставщиками телекоммуникационных услуг по вопросам, связанным с ИБ.

7.6.2 Во взаимодействии с работниками отдела АСУ:

защита Активов в соответствии с мерами по ИБ;

прогнозирование, предупреждение и выявление инцидентов ИБ, реагирование на них;

регистрация нарушений ИБ, анализ и обобщение информации о них, ведение базы инцидентов ИБ, разработка процедур реагирования на инциденты;

управления доступом к определённой ИС (ресурсу)

7.7. Представители поставщиков услуг имеют обязательства по вопросам ИБ в рамках договорных отношений.

7.8. Работникам отдела АСУ предоставляются права доступа к ИС (ресурсам), в объеме, необходимом и достаточном для выполнения возложенных на них обязанностей.

7.9. Настройка параметров доступа пользователей к ИС (ресурсу) в интересах обеспечения защиты информации выполняются работником отдела АСУ по предварительному согласованию с заместителем директора по безопасности, режиму и кадрам (специалистом по защите информации).

7.10. Начальник отдела АСУ обеспечивает поддержание в рабочем состоянии Активов, и осуществляет:

назначение (изменение) или блокирование при обнаружении нарушений прав доступа пользователя к ИС (ресурсу), по согласованию со специалистом по защите информации;

анализ событий безопасности с целью выявления нарушений безопасности Активов или попыток несанкционированных действий в ИС;

ведение базы инцидентов ИБ;

восстановление безопасного состояния Активов в случае нарушения их работы;

анализ рисков нарушения ИБ Активов и выработку предложений по их снижению;

контроль работы подчиненных по вопросам соблюдения требований ИБ;

информирование специалиста по защите информации обо всех инцидентах, связанных с нарушением ИБ, выявленных в ИС (ресурсах);

подготовку предложений по развитию и модернизации СЗИ, а также разработке процедур реагирования на инциденты в ИС.

7.11. Администратор сети отдела АСУ отвечает за конфигурирование ИТ-инфраструктуры, мониторинг, обеспечение доступности Активов для авторизованных пользователей в рамках их полномочий и осуществляет:

обеспечение предоставления доступа к Активам;

контроль состояния ИС (ресурса) по ключевым показателям в процессе эксплуатации;

поддержание безопасного состояния ИС (ресурса);

обеспечение создания резервных копий информационной системы (ресурса) и архивных файлов;

восстановление нормального функционирования ИС (ресурса) в случае нарушения;

контроль и своевременное блокирование действий пользователей, которые могут нарушить нормальное функционирование ИС (ресурса);

анализ записей аудита ИС (ресурса);

обеспечение функционирования и модернизации серверного, коммуникационного оборудования и средств вычислительной техники;

подготовку предложений по развитию и модернизации ИС (ресурса).

7.12. Работники Центра (пользователи ИС) обязаны:

соблюдать установленные требования и правила ИБ;

содействовать выявлению и предотвращению реализации угроз ИБ;

содействовать предупреждению и выявлению инцидентов ИБ, а также минимизации их последствий (локализации) их негативного воздействия на Активы;

незамедлительно информировать руководителя структурного подразделения и специалиста по защите информации о предполагаемых угрозах и возможных инцидентах ИБ.

8 ПОРЯДОК ВЗАИМОДЕЙСТВИЯ С ИНЫМИ ИНФОРМАЦИОННЫМИ СИСТЕМАМИ И СЕТЯМИ

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

8.2. При подготовке проектов договоров, предусматривающих доступ сторонних организаций (информационных систем) к ИС и (или) ее компонентам, необходимо учитывать следующие вопросы:

обязательства о конфиденциальности;

разрешенные способы доступа, а также использование и контроль за использованием уникальных идентификаторов пользователей и паролей;

наименование каждого предоставляемого информационного ресурса;

право отслеживать действия пользователей;

ограничение на копирование информации;

применение сертифицированных средств канального (линейного) шифрования;

меры по обеспечению защиты от вредоносного программного

обеспечения.

8.3. Глобальная компьютерная сеть Интернет в деятельности Центра используется в целях:

организации доступа к ИС;

получения и распространения информации, связанной с деятельностью Центра через официальный сайт;

информационно-аналитической работы;

обмена служебными электронными сообщениями.

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

9 ОТВЕТСТВЕННОСТЬ

9.1. Ответственность за поддержание положений настоящей Политики ИБ в актуальном состоянии, создание, внедрение, поддержку, мониторинг, анализ, координацию и внесение улучшений в процессы обеспечения ИБ несет специалист по защите информации.

9.2. Требования по обеспечению ИБ должны неукоснительно соблюдаться работниками Центра в порядке, определенном законодательством Республики Беларусь и положениями ЛПА, в части касающейся ИБ.

9.3. Контроль за соблюдением работниками требований ЛПА по защите информации и положений настоящей Политики осуществляет заместитель директора по безопасности, режиму и кадрам (в рамках должностных обязанностей) и специалист по защите информации.

9.4. Ответственность работников Центра и представителей иных организаций, получивших доступ к Активам в рамках договорных обязательств, за невыполнение требований ЛПА по защите информации и положений настоящей Политики определяется в соответствии с законодательством Республики Беларусь.

10 ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

10.1. Пересмотр и корректировка положений настоящей Политики осуществляется на периодической и внеплановой основе.

10.2. Плановый пересмотр настоящей Политики ИБ должен выполняться не реже одного раза в год.

10.3. Внеплановый пересмотр настоящей Политики ИБ выполняется в следующих случаях:

изменения законодательства в области защиты информации;

изменения технических НПА в области защиты информации;

существенных изменений организационной или технологической инфраструктуры, а также условий ее эксплуатации;

решение директора Центра.

Приложение
к Политике информационной
безопасности РНПЦ детской
хирургии

Перечень
частных политик в области информационной безопасности

1. Политика создания, защиты и использования паролей в государственном учреждении «Республиканский научно-практический центр детской хирургии».

2. Политика доступа к объектам системы защиты информации информационных систем в государственном учреждении «Республиканский научно-практический центр детской хирургии».

3. Политика учетных записей работников в государственном учреждении «Республиканский научно-практический центр детской хирургии».

4. Политика использования глобальной компьютерной сети Интернет и служебной электронной почты в государственном учреждении «Республиканский научно-практический центр детской хирургии».