Приложение к приказу
ФГБУ «НМИЦ детской травматологии
и ортопедии имени Г.И. Турнера»
Минздрава России
от «06» марта 2025 г. № 132

ПОЛИТИКА
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
федерального государственного бюджетного учреждения "Национальный медицинский исследовательский центр детской травматологии и ортопедии имени Г.И. Турнера" Министерства здравоохранения Российской Федерации

Содержание

целям деятельности и предназначены для снижения рисков до приемлемого уровня.

Реализация и контроль исполнения требований, установленных настоящей Политикой, осуществляется работниками, ответственными за ИБ, в соответствии со своими должностными инструкциями и другими внутренними документами Центра по ИБ.

2. Термины и определения.

Администратор безопасности – функциональная роль в информационной системе, отвечающая за информационную безопасность в этой системе и имеющая право назначать иные роли и распределять права доступа.

Безопасность информации - состояние защищённости информации, обрабатываемой средствами вычислительной техники или автоматизированной системы от внутренних или внешних угроз.

Государственная тайна - защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной, оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности государства.

Доступ к информации - возможность получения информации и её использования.

Защита информации - деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Информационная безопасность – в рамках данного документа под информационной безопасностью понимается непрерывный во времени процесс обеспечения конфиденциальности (кроме информации, конфиденциальность которой не определена ни на государственном уровне, ни на локальном), целостности и доступности защищаемой информации.

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих её обработку информационных технологий и технических средств.

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Информационный процесс - процесс получения, создания, сбора, обработки, накопления, хранения, поиска, распространения и использования информации.

Информация - сведения (сообщения, данные) независимо от формы их представления.

Инцидент информационной безопасности (Инцидент ИБ) - единичное, нежелательное или неожиданное событие информационной безопасности (или совокупность таких событий), которое может скомпрометировать бизнес-процессы Центра или угрожает ее информационной безопасности.

Коммерческая тайна - научно-техническая, технологическая, производственная, финансово-экономическая или иная информация, в том числе составляющая секреты производства (ноу-хау), которая имеет действительную или потенциальную коммерческую

1. Общие положения.

Настоящая Политика информационной безопасности (далее - Политика) является внутренним документом верхнего уровня в системе организационно – распорядительной документации обеспечивающей защиту информации в информационных системах (далее – ИС) федерального государственного бюджетного учреждения «Национальный медицинский исследовательский центр детской травматологии и ортопедии имени Г.И. Турнера» Министерства здравоохранения Российской Федерации (далее – Центр), размещенным в открытом доступе на официальном сайте Центра и доступным всем сотрудникам и всем пользователям сети интернет. Представляет собой совокупность официально принятых руководством Центра систему взглядов и управленческих решений на обеспечение информационной безопасности (далее – ИБ) Центра.

Политика определяет направления деятельности сотрудников Центра по устранению потенциальных угроз ИБ в процессе научной, образовательной, исследовательской и медицинской деятельности Центра, содержит цели, задачи и принципы достижения требуемого уровня защиты информации, определяет виды угроз ИБ в информационных системах Центра.

Основу политики ИБ составляет:

- соответствие процессов сбора, накопления, обработки, предоставления и распространения информации требованиям Указов Президента Российской Федерации, законодательства Российской Федерации, постановлениям Правительства Российской Федерации, требованиям и нормативным документам регуляторов (ФСТЭК, ФСБ, РКН России), а также внутриведомственным требованиям Министерства здравоохранения и Министерства науки и образования;
- единство мнений руководства Центра в области реализации технических, программных и организационно-распорядительных мер по защите информационных систем и технологий;
- централизованная разработка документов Центра, регламентирующих вопросы ИБ и обязательность выполнения их требований;
- обеспечение постоянного контроля состояния ИБ в Центре.
- персональная ответственность сотрудников Центра за нарушения в сфере ИБ;

Информация, обрабатываемая и используемая в Центре, является одним из ценных активов, и, следовательно, нуждается в соответствующей защите. Несанкционированное изменение, блокирование, нарушение целостности и недоступности информации может привести к нарушению жизнедеятельности Центра его научной, образовательной, исследовательской и медицинской деятельности, также несанкционированный доступ к информации, ограниченность доступа к которой определена руководством Центра и(или) требованиями законодателя и регуляторов, может явится причиной материального ущерба для Центра его контрагентов участвующих в обеспечении жизнедеятельности Центра.

В рамках своей деятельности Центр стремится предпринимать все возможные технические и организационные меры для защиты информации от риска причинения вреда, убытков и ущерба, возникающих в результате реализации угроз информационной безопасности или других противоправных действий, связанных с нарушением информационной безопасности в Центре.

Требования к обеспечению ИБ, которые предъявляются в Центре, соответствуют

ценность в силу неизвестности её третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введён режим коммерческой тайны.

Контролируемая зона - это пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание сотрудников и посетителей организации, а также транспортных средств.

Конфиденциальная информация - информация с ограниченным доступом, за исключением сведений, отнесённых к государственной тайне и персональным данным, содержащейся в информационных системах Центра, накопленная за счёт Центра и являющейся собственностью Центра (к ней может быть отнесена информация, составляющая служебную тайну и другие виды тайн в соответствии с законодательством Российской Федерации, а также сведения конфиденциального характера в соответствии с «Перечнем сведений конфиденциального характера», утверждённого Указом Президента Российской Федерации от 06.03.1997 №188), защита которой осуществляется в интересах Центра.

Конфиденциальность персональных данных - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

Модель угроз (безопасности информации) - физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации.

Мультисервисная сеть - универсальная многоцелевая среда, предназначенная для передачи речи, изображения и данных с использованием технологии коммутации пакетов.

Несанкционированный доступ к информации – доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами информационных систем.

Носитель защищаемой информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит своё отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обработка персональных данных – любое действие (операция) или совокупность действий, совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (в том числе распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующее и (или) осуществляющее обработку персональных данных, а также определяющее цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Персональные данные - любая информация, относящаяся прямо или косвенно к определённому или определяемому физическому лицу (субъекту персональных данных).

Подсистема информационной безопасности – структурная часть общей системы информационной безопасности Центра. Подсистема информационной безопасности служит для реализации технических защитных мер в отношении: отдельной

информационной системы; сети передачи данных или её сегмента; автоматизированного рабочего места; конкретной категории защищаемой информации.

Режим коммерческой тайны - режим конфиденциальности информации, позволяющий её обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

Сертификация на соответствие требованиям по безопасности информации - форма осуществляемого органом по сертификации подтверждения соответствия объектов оценки требованиям по безопасности информации, установленным техническими регламентами, стандартами или условиями договоров.

Средство защиты информации - техническое и(или) программное средство предназначенное или используемое для защиты информации.

Система обеспечения информационной безопасности - функционирующая как единое целое совокупность средств и мероприятий, и применяемых при проведении мероприятий мер, устремлённая на ликвидацию внутренних и внешних угроз жизненно важным интересам субъекта безопасности, создание, поддержание и развитие состояния защищённости его информационной среды.

3. Список использованных сокращений.

1. **АРМ** – автоматизированное рабочее место.
2. **ИС** – информационная система.
3. **АС** – автоматизированная система.
4. **ИСПДн** – информационная система, содержащая персональные данные.
5. **КЗ** – контролируемая зона.
6. **КТ** – коммерческая тайна; информация, составляющая коммерческую тайну.
7. **МСС** – мультисервисная сеть.
8. **ОИТ** – отдел информационных технологий.
9. **ОС** – операционная система.
10. **НСД –** несанкционированный доступ к информации.
11. **ПДн** – персональные данные.
12. **ПИБ** – подсистема информационной безопасности.
13. **ПО** – программное обеспечение.
14. **Пользователи ИС** – сотрудники Центра, использующие в процессе выполнения своих должностных обязанностей те или иные информационные системы Центра.
15. **ОРД** – организационно-распорядительная документация.
16. **СВТ** – средство вычислительной техники.
17. **СУИБ** – система управления информационной безопасности.
18. **СКЗИ**– средство криптографической защиты информации.
19. **СТР-К** - Специальные требования и рекомендации по технической защите конфиденциальной информации одобренные решением коллегии Гостехкомиссии России от 02.03.2001 г.
20. **ТЗ** – техническое задание.
21. **ФСБ России** – Федеральная служба безопасности Российской Федерации.
22. **ФСТЭК России** – Федеральная служба по техническому и экспортному контролю Российской Федерации.

23. **РКН** - Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)

4. Цели и задачи политики информационной безопасности.

Политика представляет собой систематизированное изложение целей и задач защиты, основных принципов построения системы ИБ, требований к организационным и техническим мерам защиты информации в ИС Центра.

Целями обеспечения информационной безопасности Центра являются:

- защита интересов Центра и иных субъектов, взаимодействующих с Центром с использованием информационных технологий, от возможного нанесения вреда их деятельности посредством случайного или преднамеренного несанкционированного доступа и вмешательства в процесс функционирования ИС Центра, приводящего к блокировке, разглашению, искажению, уничтожению защищаемой информации или ее незаконному использованию;
- обеспечение устойчивого функционирования технических и программно-аппаратных комплексов ИС Центра обеспечивающих взаимодействие Центра со всеми участниками информационного обмена;
- выполнение требований действующего законодательства, приказов и методических рекомендаций профильных регуляторов в области информационной безопасности;
- разработка и внедрение внутренней организационно – распорядительной документации на основе принципов, изложенных в настоящей Политики регламентирующих правила и нормы информационной безопасности.

Для достижения поставленных целей необходимо обеспечивать эффективное решение следующих задач:

- своевременное выявление, оценка и прогнозирование источников угроз ИБ;
- создание механизма оперативного реагирования на угрозы ИБ;
- предотвращение и/или снижение ущерба от реализации угроз ИБ;
- защита от вмешательства в процесс функционирования ИС посторонних лиц;
- соответствие требованиям Федерального законодательства, нормативно-методических документов ФСБ России, ФСТЭК России и договорным обязательствам в части ИБ;
- обеспечение непрерывности критических бизнес-процессов;
- достижение адекватности мер по защите от угроз ИБ;
- изучение и оценка действий сотрудников;
- повышение деловой репутации и корпоративной культуры.

5. Принципы политики информационной безопасности

Для достижения поставленных целей Центр руководствуется следующими принципами:

Принцип законности. Предполагает осуществление защитных мероприятий и разработку системы безопасности информации в соответствии с действующим законодательством в области информации, информационных технологий и защиты информации, а также других нормативных актов по безопасности, утверждённых органами государственной власти.

Принцип системности. Системный подход к защите информации в Центре предполагает учёт всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения информационной безопасности в Центре. При создании системы защиты должны учитываться все слабые и наиболее уязвимые места системы обработки информации, а также характер, возможные объекты и направления атак на систему со стороны нарушителей, пути проникновения в распределённые системы и НСД к информации. Система защиты должна строиться с учётом не только всех известных каналов проникновения и НСД к информации, но и с учётом возможности появления принципиально новых путей реализации угроз безопасности.

Принцип Комплексности. Комплексное использование методов и средств защиты компьютерных систем предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные (значимые) векторы угроз информационной безопасности и не содержащей слабых мест на стыках отдельных её компонентов. Защита должна строиться эшелонировано. Внешняя защита ИС должна обеспечиваться физическими средствами, организационными, технологическими и правовыми мерами. Одним из наиболее укреплённых рубежей призваны быть средства защиты, реализованные на уровне операционных систем СВТ в силу того, что ОС - это та часть компьютерной системы, которая управляет использованием всех её ресурсов. Прикладной уровень защиты, учитывающий особенности предметной области, представляет внутренний рубеж защиты.

Принцип непрерывности защиты. Защита информации - непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла ИС Центра, начиная с самых ранних стадий проектирования, а не только на этапе её эксплуатации. Большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имён, паролей, ключей шифрования, переопределение полномочий и т.п.). Перерывы в работе средств защиты могут быть использованы злоумышленниками для внедрения специальных программных и аппаратных «закладок» и других средств преодоления системы защиты после восстановления её функционирования.

Принцип своевременности. Предполагает упреждающий характер мер обеспечения безопасности информации, то есть постановку задач по комплексной защите ИС Центра и реализацию мер обеспечения безопасности информации на ранних стадиях разработки ИС в целом и её системы информационной безопасности, в частности. Разработка системы защиты должна вестись параллельно с разработкой и развитием самой защищаемой системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счёте, создать более эффективные (как по затратам ресурсов, так и по стойкости) защищённые системы.

Принцип преемственности и совершенствования. Предполагают постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, анализа функционирования информационных систем и их систем информационной безопасности с учётом изменений в методах и средствах перехвата информации и воздействия на компоненты ИС, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.

Принцип разумной достаточности (экономическая целесообразность, сопоставимость возможного ущерба и затрат). Предполагает соответствие уровня затрат на обеспечение безопасности информации ценности информационных ресурсов, величине возможного ущерба от их разглашения, утраты, утечки, уничтожения и искажения. Используемые меры и средства обеспечения безопасности информационных ресурсов не должны заметно ухудшать экономические показатели работы ИС Центра, в которых эта информация циркулирует. Важно правильно выбрать тот достаточный уровень защиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми (задача анализа риска).

Принцип персональной ответственности. Предполагает возложение ответственности за обеспечение безопасности информации и системы её обработки на каждого сотрудника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей сотрудников строится таким образом, чтобы в случае любого нарушения круг виновных лиц был чётко известен или сведён к минимуму.

Принцип минимизации полномочий. Означает предоставление пользователям минимальных прав доступа в соответствии со служебной необходимостью. Доступ к информации должен предоставляться только в том случае и объёме, в каком это необходимо сотруднику для выполнения его должностных обязанностей.

Принцип открытости алгоритмов и механизмов защиты. Суть принципа открытости алгоритмов и механизмов защиты состоит в том, что защита не должна обеспечиваться только за счёт секретности структурной организации и алгоритмов функционирования её подсистем. Знание алгоритмов работы системы защиты не должно давать возможности её преодоления (даже авторам). Это, однако, не означает, что информация о конкретной системе защиты должна быть общедоступна.

Принцип специализации и профессионализма. Предполагает привлечение к разработке средств и реализации мер защиты информации сотрудников, имеющих соответствующее образование и опыт. Реализация административных мер и эксплуатация средств защиты также должна осуществляться профессионально подготовленными сотрудниками (специалистами отвечающих за безопасности информации).

Принцип обязательности контроля. Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности информации на основе используемых систем и средств защиты информации. Контроль за деятельностью любого пользователя, каждого средства защиты и в отношении любого объекта защиты должен осуществляться на основе применения средств оперативного контроля и регистрации, должен охватывать как несанкционированные, так и санкционированные действия пользователей.

Принцип вовлеченности руководства. Деятельность по обеспечению информационной безопасности инициирована и контролируется руководством Центра. Руководство Центра следует тем же правилам по обеспечению информационной безопасности, как и все сотрудники Центра.

6. Основания для разработки

Политика разработана на основе требований законодательства Российской Федерации, накопленного в Центре опыта в области защиты информационных ресурсов, интересов Центра и его целей.

При написании отдельных положений настоящей политики использовались следующие нормативные документы:

ГОСТ Р ИСО/МЭК 27001 «Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности»;

ГОСТ Р ИСО 7498-2-99 «Информационная технология. Архитектура защиты информации»;

ГОСТ Р 50922-96 Защита информации. Основные термины и определения;

Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

7. Область действия

Настоящая Политика распространяется на все бизнес-процессы и информационные системы Центра и обязательна для применения всеми сотрудниками и руководством Центра в повседневной деятельности, а также пользователями информационных ресурсов Центра.

Сотрудники, ведущие разработку и внедрение внутренних документов Центра, регламентирующих вопросы ИБ, должны руководствоваться настоящей Политикой.

8. Содержание Политики

8.1. Система управления информационной безопасности

Для достижения целей и задач, указанных в Политике, Центр внедряет систему управления информационной безопасностью (далее – СУИБ).

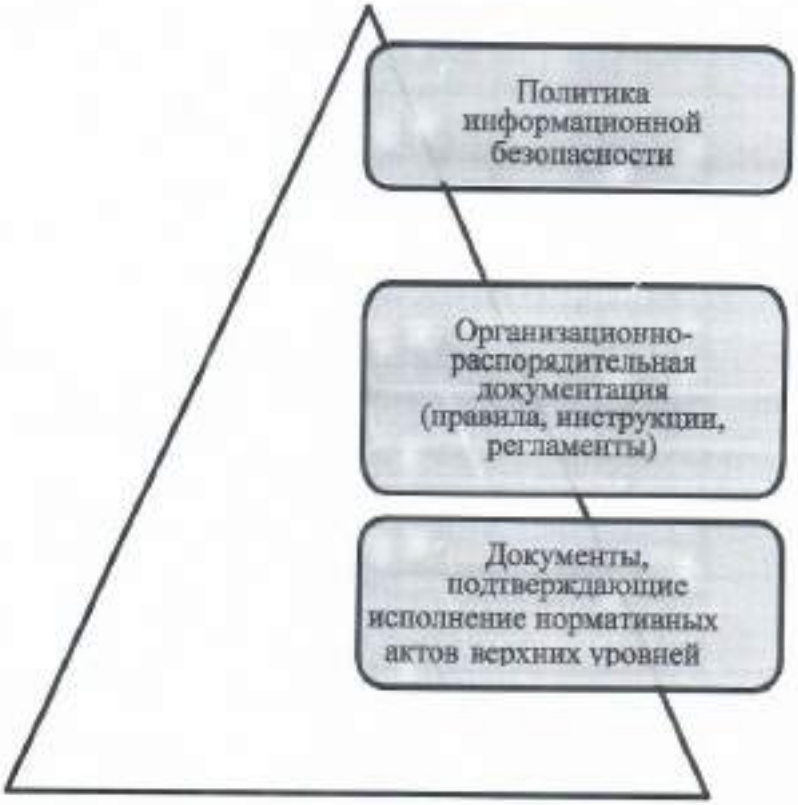
Требования системы управления информационной безопасности документально утверждены в организационно-распорядительных документах, которые являются обязательными для всех работников Центра в области ИБ. Документы с требования СУИБ доводятся до сведения работников Центра.

СУИБ внедряются и редактируется по результатам периодически проводимого анализа оценки рисков ИБ.

Стоимость внедряемых технических средств информационной безопасности не должна превышать размер возможного ущерба, возникшего при реализации угроз ИБ.

8.1.1. Иерархия документов

В целях создания взаимосвязанной вертикали нормативных документов Учреждения в области обеспечения ИБ, разрабатываемые и обновляемые нормативные документы должны соответствовать следующей иерархии:



1. Политика является внутренним нормативным документом Центра в области информационной безопасности первого уровня.
2. Правила, инструкции, регламенты и прочие документы, описывающие действия сотрудников Центра при реализации требований документов первого и второго уровня.
3. Документы третьего уровня – это документы, подтверждающие исполнение ОРД верхних уровней.

8.1.2. Ответственность за управление ИБ

Функции по управлению ИБ в Центре возложены на отдел информационных технологий.

Отдел информационных технологий решает следующие основные задачи:

- разработку и внедрение Политики ИБ в Центре;
- определение требований к защите информации;
- организация мероприятий и координация работ всех подразделений по вопросам комплексной защиты информации;
- контроль и оценка эффективности принятых мер и применяемых средств защиты;
- оказание методической помощи сотрудникам в вопросах обеспечения ИБ;
- регулярная оценка и управление рисками ИБ в соответствии с установленными процедурами;
- выбор и внедрение средств защиты информации, включая организационные, физические, технические, программные и программно-аппаратные средства обеспечения СУИБ;
- обеспечение минимально-необходимого доступа к информационным ресурсам, основываясь на требованиях бизнес-процессов;

• информирование, обучение и повышение квалификации работников Центра в сфере ИБ;

• расследования инцидентов ИБ;

• сбор, накопление, систематизация и обработка информации по вопросам ИБ;

• обеспечение необходимого уровня отказоустойчивости ИС и доступности данных для структурных подразделений.

Для решения задач, возложенных на отдел информационных технологий, его сотрудники, отвечающие за ИБ, имеют следующие права:

• выявлять необходимость в нормативных документах и осуществлять их разработку, касающиеся вопросов обеспечения безопасности информации, включая документы, регламентирующие деятельность пользователей ИС в области ИБ;

• получать информацию от пользователей ИС Центра по любым аспектам применения информационных технологий в Центре;

• участвовать в проработке новых технических решений по вопросам обеспечения безопасности информации в информационных системах Центра;

• участвовать в испытаниях новых технических решений и оценки качества обеспечения безопасности информации;

• контролировать деятельность пользователей в вопросах соблюдения требований ИБ;

• готовить предложения руководству по обеспечению требований ИБ.

8.2. Защищаемая информация, информационные системы и ответственность за информационные системы

Центр определяет и оценивает важность всех имеющихся у него информационных систем. Важные ИС должны быть учтены в едином реестре информационных систем Центра. Имея информацию о важности ИС, Центр реализует защиту информации в ИС, степень которой соразмерна степени важности информации, содержащейся в ИС.

Для каждой ИС должен быть назначен владелец, который отвечает за полноту и достоверность циркулирующей в ИС информации. Владелец информации также отвечает за назначение и периодическую проверку прав доступа и категорий должностных лиц, допущенных к ИС. Периодически информация в ИС должна пересматриваться и (или) дополнятся для поддержания её актуальности.

ИС содержащие конфиденциальную информацию, и/или сведения ограниченного доступа, в том числе информацию о состоянии здоровья пациентов Центра должны иметь соответствующую пометку.

8.3. Оценка рисков

Оценка рисков — это общий процесс идентификации, анализа и определения приемлемости уровня риска ИБ Центра.

Кроме того, оценка рисков и выбор механизмов контроля должны производиться периодически, чтобы:

• учесть изменения требований и приоритетов;

• принять во внимание новые угрозы и уязвимости;

• убедиться в том, что реализованные средства сохранили свою эффективность.

Перед обработкой каждого риска руководство Центра должно выбрать критерии для определения возможности принятия этого риска. Риск может быть принят, если его величина достаточно мала и стоимость обработки нерентабельна для Центра.

Для каждого из оцененных рисков должно приниматься одно из решений по его обработке:

• применение соответствующих механизмов контроля для уменьшения величины риска до приемлемого уровня;

• сознательное и объективное принятие риска, если он точно удовлетворяет Политике Центра и критериям принятия рисков;

• уклонение от риска путём недопущения действий, которые могут стать его причиной;

• передача рисков другой стороне (аутсорсинг, страхование и т.п.).

8.4. Обязанности персонала

Обязанности по обеспечению безопасности информационных систем, описанные в соответствии с настоящей Политикой, должны быть доведены до сотрудника при трудоустройстве путём заключения соглашения о конфиденциальности. В соглашение о конфиденциальности входят как общие обязанности по реализации и поддержке Политики, так и конкретные обязанности по защите информации и по выполнению конкретных операций, связанных с информационной безопасностью.

8.4.1. Условия найма

Все принимаемые на работу сотрудники должны подписать свои трудовые договоры, а также соглашение о конфиденциальности в котором устанавливается их ответственность за ИБ. В договор должно быть включено согласие сотрудника на проведение контрольных мероприятий со стороны Центра по проверке выполнения требований ИБ. В соглашении о конфиденциальности указаны обязательства по неразглашению конфиденциальной информации и описаны меры, которые будут приняты в случае несоблюдения сотрудником требований ИБ. Обязанности по обеспечению ИБ включены в согласие о конфиденциальности.

Все принимаемые сотрудники должны быть ознакомлены под подпись с перечнем информации ограниченного доступа, с установленным режимом обращения с ней и с мерами ответственности за нарушение этого режима. При предоставлении сотруднику доступа к ИС Центра он должен ознакомиться под подпись с инструкцией пользователя ИС.

8.4.2. Проведение проверок

Уполномоченные руководством Центра сотрудники имеют право в установленном порядке, без уведомления пользователей, производить проверки:

• выполнения действующих инструкций по вопросам ИБ;

• данных, находящихся на носителях информации;

• порядка использования сотрудниками информационных систем;

• содержания служебной переписки.

8.4.3. Завершение или изменения трудовых отношений

При увольнении все предоставленные сотруднику права доступа к ресурсам ИС должны быть удалены. При изменении трудовых отношений удаляются только те права, необходимость в которых отсутствует в новых отношениях.

8.5. Физическая безопасность

8.5.1. Защищённые помещения

Средства обработки информации, поддерживающие критически важные и уязвимые ИС Центра, должны быть размещены в защищённых помещениях. Такими средствами

являются: серверы, магистральное телекоммуникационное оборудование, телефонные станции, кроссовые панели, оборудование, обеспечивающее обработку и хранение персональных данных пациентов и сотрудников и другой конфиденциальной информации.

Защищённые помещения должны оборудоваться соответствующими средствами контроля доступа, обеспечивающими возможность доступа только авторизованного персонала.

Для хранения служебных документов и машинных носителей с защищаемой информацией, помещения должны быть снабжены сейфами, металлическими шкафами или шкафами, оборудованными замком.

8.5.2. Утилизация оборудования

Со всех носителей информации, которыми укомплектовано утилизируемое оборудование, должны гарантированно удаляться все информация и лицензионное ПО. Отсутствие защищаемой информации на носителях должно быть проверено отделом ИТ Центра, о чём должна быть сделана отметка в акте списания.

8.5.3. Перемещение имущества

Оборудование, информация или ПО должны перемещаться за физические границы Центра только при наличии письменного разрешения руководства Центра. Должны быть определены сотрудники, имеющие право выноса оборудования и носителей информации за пределы физической границы Центра. Данные о выносе оборудования за пределы физической границы Центра и его возврата должны регистрироваться в журнале учета носителей и мобильного оборудования.

8.6. Контроль доступа

Основными пользователями ИС Центра являются сотрудники структурных подразделений Центра. Уровень полномочий каждого пользователя определяется индивидуально. Каждый сотрудник пользуется только предписанными ему правами по отношению к информации, с которой ему необходимо работать в соответствии с должностными обязанностями.

Допуск пользователей к работе в ИС должен быть строго регламентирован. Любые изменения состава и полномочий пользователей должны производиться в установленном порядке, согласно разрабатываемой владельцем информации матрице доступа.

Каждому пользователю, допущенному к работе с конкретными ИС Центра, должно быть присвоено персональное уникальное имя (учётная запись пользователя), под которым он будет авторизовываться и работать с той или иной ИС.

В случае производственной необходимости некоторым сотрудникам могут быть присвоены несколько уникальных имён (учётных записей).

Временная учетная запись может быть заведена для пользователя на ограниченный срок для выполнения задач, требующих расширенных полномочий, или для проведения настройки, тестирования ИС, для организации гостевого доступа (посетителям, сотрудникам сторонних организаций, стажерам и иным пользователям с временным доступом к ИС).

Запрещено создавать и использовать общую пользовательскую учётную запись для группы пользователей.

Регистрация и блокирование учётных записей пользователей должны применяться с соблюдением следующих правил:

• использование уникальных идентификаторов (ID) пользователей для однозначного определения и сопоставления личности с совершёнными ей действиями;

• предоставление и блокирование прав должны быть санкционированы и документированы;

• предоставление прав доступа к ИС, только после согласования с владельцем, данной ИС;

• регистрация и блокирование учётных записей допускается после согласования с начальником отдела информационных технологий, по заявке руководителя структурного подразделения;

• уровень предоставленных полномочий должен соответствовать производственной необходимости и настоящей Политике;

• согласование изменения прав доступа с начальником отдела информационных технологий;

• документальная фиксация назначенных пользователю прав доступа;

• ознакомление пользователей под подпись, с письменными документами (как правило должностные инструкции, соглашение о конфиденциальности), в которых регламентируются их права доступа;

• предоставление доступа с момента завершения процедуры регистрации;

• создание и поддержание в актуальном состоянии списка всех пользователей, зарегистрированных для работы в ИС;

• регулярный аудит учетных записей пользователей на наличие неиспользуемых, их дальнейшее удаление и блокировка после согласования с начальником отдела ИТ;

• обеспечение того, чтобы личные ID пользователей не были доступны другим пользователям;

В случаях изменения должности сотрудника, формы занятости или увольнения из Центра, руководитель подразделения в распоряжении которого находился сотрудник, уведомляет начальника отдела ИТ об изменениях, для блокирования или модификации учетной записи.

8.6.1. Управление привилегиями

Доступ сотрудника к ИС Центра должен быть санкционирован руководителем структурного подразделения, в котором числится, согласно штатному расписанию, данный сотрудник, и владельцем соответствующих ИС. Управление доступом осуществляется в соответствии с установленными процедурами.

Наделение привилегиями и их использование должно быть строго ограниченным и управляемым. Распределение привилегий должно управляться с помощью процесса регистрации этих привилегий. Должны быть рассмотрены следующие этапы:

• идентификация привилегии доступа, связанная с каждым системным продуктом, например, с операционной системой, системой управления базой данных и каждым приложением, а также с пользователями, которым они предоставлены;

• привилегии предоставляются пользователям на основании «производственной необходимости» и только на период времени, необходимый для достижения поставленных целей, например, привилегии, минимально необходимые для выполнения их функциональных обязанностей, только тогда, когда эти привилегии необходимы;

• обеспечение процесса санкционирования всех предоставленных привилегий и создание отчетов по ним;

• уникальные привилегии присваиваются на другой ID пользователя, не тот, который используется при обычной работе пользователя.

Контроль и периодический пересмотр прав доступа пользователей к информационным ресурсам Центра осуществляется в процессе аудита ИБ в соответствии с Правилами аудита ИБ и установленными процедурами.

8.6.2. Управление паролями

Предоставление паролей должно контролироваться посредством официальной процедуры, отвечающей следующим требованиям:

• все пользователи должны быть ознакомлены под подпись с требованием сохранения в тайне личных паролей;

• при наличии возможности, необходимо настроить систему таким образом, чтобы при первом входе пользователя с назначенным ему временным паролем система сразу же требовала его сменить;

• временные пароли должны назначаться пользователю только после его идентификации;

• необходимо запрещать передачи паролей с использованием третьих лиц или незашифрованной электронной почтой;

• временные пароли не должны быть угадываемыми и повторяющимися от пользователя к пользователю;

• пароли должны храниться в электронном виде только в защищенной форме;

• назначенные производителем ПО пароли должны быть изменены сразу после завершения инсталляции;

• необходимо установить требования к длине пароля, сроку действия, набору символов и числу попыток ввода;

• при наличии возможности, необходимо настроить систему таким образом, чтобы пользователь изменял пароль не реже одного раза в 90 дней.

При необходимости можно рассмотреть возможность использования других технологий идентификации и аутентификации пользователей, в частности, биометрических технологий, проверки подписи и аппаратных средств (смарт-карты, e-Token/ruToken, чипы и т.п.).

8.6.3 Использование паролей

Идентификатор и пароль пользователя в ИС являются учётными данными, на основании которых сотруднику Центра предоставляются права доступа, протоколируются производимые им в системе действия и обеспечивается режим конфиденциальности, обрабатываемой (создаваемой, передаваемой, редактируемой и хранимой) сотрудником информации. Не допускается использование различными пользователями одних и тех же учётных данных.

После первого входа в систему и в дальнейшем, пароли создаются пользователями самостоятельно с учетом следующих требований:

• длина пароля должна быть не менее 8 символов;

• в числе символов пароля должны присутствовать три из четырёх видов символов:

- буквы в верхнем регистре;
- буквы в нижнем регистре;
- цифры;
- специальные символы (! @ # $ % ^ & * ( ) - _ + = ~ [ ] { } | \ : ; ' " < > , . ? /);

• пароль не должен содержать легко вычисляемые сочетания символов, например:

- имена, фамилии, номера телефонов, даты;
- последовательно расположенные на клавиатуре символы («12345678», «QWERTY», и т.д.);
- общепринятые сокращения («USER», «TEST» и т.п.);
- повседневно используемое слово, например, имена или фамилии друзей, коллег, актёров или сказочных персонажей, клички животных;

- компьютерный термин, команда, наименование компаний, web сайтов, аппаратного или программного обеспечения;

- что-либо из вышеперечисленного в обратном написании;

- что-либо из вышеперечисленного с добавлением цифр в начале или конце;

• при смене пароля значение нового должно отличаться от предыдущего не менее чем в 4 позициях;

• для различных ИС необходимо устанавливать собственные, отличающиеся пароли.

Сотруднику рекомендуется выбирать пароль с помощью следующей процедуры:

• выбрать фразу, которую легко запомнить. Например, «Три мудреца в одном тазу пустились по морю в грозу»;

• выбрать первые буквы из каждого слова «тмвотппмвг»;

• набрать полученную последовательность, переключившись на английскую раскладку клавиатуры: «nvdjnggvdu»;

• выбрать номер символа, который будет записываться в верхнем регистре и после которого будет специальный символ. Например, это будет пятый символ, а в качестве специального символа выбран «#». Получаем: «nvdjN#ggvdu».

Сотруднику запрещается:

• сообщать свой пароль кому-либо;

• указывать пароль в сообщениях электронной почты;

• хранить пароли, записанные на бумаге, в легко доступном месте;

• использовать тот же самый пароль, что и для других систем (например, домашний интернет - провайдер, бесплатная электронная почта, форумы и т.п.);

• использовать один и тот же пароль для доступа к различным корпоративным ИС.

Сотрудник обязан:

• в случае подозрения на то, что пароль стал кому-либо известен, поменять пароль и сообщить о факте компрометации уполномоченному сотруднику отдела ИТ;

• немедленно сообщить уполномоченному сотруднику отдела ИТ в случае получения от кого-либо просьбы сообщить пароль;

• менять пароль каждые 90 дней;

• менять пароль по требованию сотрудника ИТ.

Уполномоченные сотрудники отдела ИТ Центра наделены полномочиями:

• осуществлять периодическую проверку стойкости паролей пользователей, используемых сотрудниками для доступа к ИС;

• ходатайствовать о применении мер дисциплинарного характера к сотрудникам, нарушающим положения настоящей Политики.

8.6.4 Контроль прав доступа

Для обеспечения эффективного контроля доступа необходимо ввести официальный процесс регулярной проверки прав доступа пользователей, отвечающий следующим требованиям:

• права доступа пользователей должны проверяться через регулярные интервалы (не реже одного раза в полгода), а также после внесения каких-либо изменений в ИС;

• права доступа пользователей должны проверяться и переназначаться при изменении их должностных обязанностей, а также при переходе с одной работы на другую в пределах Центра;

• проверка прав пользователей, имеющих особые привилегии для доступа в систему, должна проводиться не реже одного раза в 3 месяца;

• необходимо регулярно проверять адекватность назначенных привилегий, во избежание получения кем-либо из пользователей излишних прав;

• изменение привилегированных учетных записей должно протоколироваться.

Контроль над выполнением процедур управления доступом пользователей должен включать:

• контроль над добавлением, удалением и изменением идентификаторов, аутентификационных данных и иных объектов идентификации;

• проверку подлинности пользователей перед сменой паролей;

• блокирование прав доступа при увольнении сотрудника, по заявке кадрового отдела, согласованной с начальником отдела информационных технологий;

• блокирование учётных записей, неактивных более 45 дней;

• включение учётных записей, используемых поставщиками для удалённой поддержки, только на время выполнения работ;

• отслеживание удалённых учётных записей, используемых поставщиками, во время работ;

• предотвращение повторного использования идентификатора пользователя и (или) устройства в течение следующих трёх лет;

• ознакомление с правилами и процедурами аутентификации всех пользователей, имеющих доступ к сведениям ограниченного распространения;

• использование механизмов аутентификации при доступе к любой базе данных, содержащей сведения ограниченного распространения, в том числе доступе со стороны приложений, администраторов и любых других пользователей;

• разрешение запросов и прямого доступа к базам данных только для администраторов баз данных;

• блокирование учётной записи на период равный 30 минутам или до разблокировки учётной записи администратором при 5 ошибках аутентификации;

• блокирование учетных записей пользователей при выявлении по результатам мониторинга (просмотра, анализа) журналов регистрации событий безопасности действий пользователей, которые отнесены оператором к событиям нарушения безопасности информации.

8.6.5 Пользовательское оборудование, оставляемое без присмотра

Пользователи должны обеспечивать необходимую защиту оборудования, остающегося без присмотра. Все пользователи должны быть осведомлены о требованиях ИБ и правилах защиты остающегося без присмотра оборудования, а также о своих обязанностях по обеспечению этой защиты.

Компьютеры и терминалы должны быть оставлены в состоянии выполненного выхода из системы, когда они находятся без присмотра.

Вход пользователя в систему не должен выполняться автоматически. Покидая рабочее место, пользователь обязан заблокировать компьютер (используя комбинации Win + «L» или Ctrl + Alt + Delete → «Блокировать компьютер»).

8.6.6 Политика чистого стола

Сотрудники Центра обязаны:

• сохранять известные им пароли в тайне;

• закрывать активные сеансы по завершении работы.

Запрещается вести запись паролей (например, на бумаге, в программном файле или в карманном устройстве).

Документы и носители с конфиденциальной информацией должны убираться в запираемые места (сейфы, шкафы и т.п.), при уходе с рабочего места. Документы, содержащие конфиденциальную информацию, должны изыматься из печатающих устройств немедленно.

В конце рабочего дня сотрудник должен привести в порядок письменный стол и убрать все офисные документы в запираемый шкаф или сейф.

Для утилизации конфиденциальных документов, должны использоваться уничтожители бумаги.

По окончании рабочего дня и в случае длительного отсутствия на рабочем месте необходимо запирать на замок все шкафы и сейфы.

8.7. Использование ПО

Общие обязанности пользователя:

• при работе с прикладным ПО руководствоваться нормативной документацией (руководством пользователя);

• обращаться в отдел ИТ или к специалистам, назначенными ответственными за системное администрирование и ИБ, а также по всем техническим вопросам, связанным с работой в локальной вычислительной сети (подключение к локальной вычислительной сети /домену, инсталляция и настройка ПО, предоставление доступа в сеть Интернет и к внутренним сетевым ресурсам, ремонт и техническое обслуживание и т.п.).

• знать признаки правильного функционирования установленных программных продуктов и средств защиты информации.

• на автоматизированных рабочих местах Центра допускается использование только лицензионное ПО.

• запрещено незаконное хранение на жестких дисках АРМ Центра информации, являющейся объектом авторского права (ПО, фотографии, музыкальные файлы, игры, и т.д.).

Решение о приобретении и установке ПО, необходимого для реализации задач принимает директор Центра по представлению начальника отдела ИТ.

Документы, подтверждающие покупку ПО, хранятся в бухгалтерии на протяжении всего времени использования лицензии, копии указанных документов вместе с лицензионными соглашениями на ПО, ключами защиты ПО и дистрибутивами хранятся в отделе ИТ.

Пользователи АРМ не имеют права удалять, изменять, дополнять, обновлять программную конфигурацию. Указанные работы, а также работы по установке, регистрации и активации приобретённого лицензионного ПО могут быть выполнены только сотрудниками отдела ИТ.

8.7.1. Использование АРМ и ИС

К работе в ИС Центра допускаются лица, назначенные на соответствующую должность и прошедшие инструктаж по вопросам ИБ.

Каждому сотруднику Центра, которому необходим доступ к ИС в рамках его должностных обязанностей, выдаются под подпись необходимые средства автоматизации. Ответственность по установке и поддержке всех компьютерных систем, функционирующих в Центре, возложена на отдел ИТ.

Каждый сотрудник Центра, получает персональное сетевое имя, пароль, адрес электронной почты.

Работа в ИС сотрудникам разрешена только на закреплённых за ними АРМ, в рабочее время и только в ИС куда им санкционирован доступ.

Все АРМ, установленные в Центре, имеют унифицированный набор офисных программ, предназначенных для обработки и обмена информацией, определённый стандартом автоматизированных рабочих мест. Изменение установленной конфигурации возможно по служебной записке, согласованной с начальником отдела ИТ.

Комплектация персональных компьютеров аппаратными и программными средствами, а также расположение компьютеров контролируется отделом ИТ.

Самостоятельная установка ПО на АРМ запрещена. Установка и удаление любого ПО производится только сотрудниками отдела ИТ.

В случае обнаружения неисправности компьютерного оборудования или ПО, пользователь должен обратиться в отдел ИТ.

Сотрудники отдела ИТ имеют право осуществлять контроль над установленным на компьютере ПО, и принимать меры по ограничению возможностей несанкционированной установки программ.

Передача документов внутри Центра производится только посредством общих папок, расположенных внутри локально вычислительной сети Центра, а также средствами электронной почты.

При работе в ИС Центра сотрудник обязан:

• знать и выполнять требования внутренних организационно-распорядительных документов Центра;

• использовать ИС и АРМ Центра исключительно для выполнения своих служебных обязанностей;

• ставить в известность отдел ИТ о любых фактах нарушения требований ИБ;

• ставить в известность отдел ИТ о любых фактах сбоев ПО, некорректного завершения значимых операций, а также повреждения технических средств;

• строго выполнять требования отдела ИТ части касающейся ИБ;

• предоставлять АРМ сотрудникам отделов ИТ для контроля;

• при необходимости прекращения работы на некоторое время корректно закрывать все активные задачи, блокировать АРМ;

• в случае необходимости продолжения работы по окончании рабочего дня проинформировать об этом отдел ИТ.

При использовании ИС Центра запрещено:

• использовать АРМ и ИС в личных целях;

• отключать средства управления и средства защиты, установленные на рабочей станции;

• передавать:

- конфиденциальную информацию за исключением случаев, когда это входит в служебные обязанности и способ передачи является безопасным, согласованным с отделом ИТ;

- информацию, файлы или ПО, способные нарушить или ограничить функциональность любых программных и аппаратных средств, а также ссылки на вышеуказанные объекты;

- угрожающую, клеветническую, непристойную информацию;

• самовольно вносить изменения в конструкцию, конфигурацию, размещение АРМ и других узлов ИС Центра;

• предоставлять сотрудникам Центра (за исключением администраторов ИС и ИБ) и третьим лицам доступ к своему АРМ;

• запускать на АРМ ПО, не входящее в реестр разрешенного к использованию ПО;

• защищать информацию, способами, не согласованными с отделом ИТ;

• самостоятельно подключать рабочую станцию и прочие технические средства к локально вычислительной сети Центра;

• осуществлять поиск средств и путей повреждения, уничтожения технических средств и ресурсов ИС или осуществлять попытки несанкционированного доступа к ним;

• использовать для выполнения служебных обязанностей локальные (не доменные) учетные записи АРМ.

Информация о посещаемых ресурсах ИС должна протоколироваться и, при необходимости, может быть представлена руководителям структурных подразделений, а также директору Центра.

Все электронные сообщения и документы в электронном виде, передаваемые посредством ИС Центра подлежат обязательной проверке на отсутствие вредоносного ПО.

8.7.2. Обработка конфиденциальной информации

При обработке конфиденциальной информации сотрудники обязаны:

- знать и выполнять требования Инструкции по работе с конфиденциальной информацией;
- размещать экран монитора таким образом, чтобы исключить просмотр обрабатываемой информации посторонними лицами;
- не отправлять на печать конфиденциальные документы, если отсутствует возможность контроля вывода на печать и изъятия отпечатанных документов из принтера сразу по окончании печати;
- обязательно проверять адреса получателей электронной почты на предмет правильности их выбора;
- не запускать исполняемые файлы на съемных накопителях, полученные не из доверенного источника;
- не передавать конфиденциальную информацию по открытым каналам связи;
- не оставлять без личного присмотра на рабочем месте или где бы то ни было электронные носители информации (CD/DVD – диски, Flash – накопители и пр.), а также распечатки из принтера или бумажные копии документов, содержащие конфиденциальную информацию.

8.7.3. Использование электронной почты

Электронная почта используется для обмена в рамках ИС Центра и общедоступных сетей информацией в виде электронных сообщений и документов в электронном виде.

При работе с корпоративной электронной почтой Центра пользователь должен учитывать:

- электронная почта не является средством гарантированной доставки отправленного сообщения до адресата;
- электронная почта не является средством передачи информации, гарантирующим конфиденциальность передаваемой информации (передачу конфиденциальной информации вне локальной сети Центра необходимо осуществлять только в зашифрованном виде);
- электронная почта не является средством передачи информации, гарантированно идентифицирующим отправителя сообщения.

Организацией и обеспечением порядка работы электронной почты в Центре занимается отдел ИТ.

Каждый сотрудник получает почтовый адрес в домене Центра. Адрес электронной почты выдаётся сотрудником отдела ИТ при начальной регистрации пользователя в домене Центра.

Корпоративная электронная почта Центра предназначена исключительно для использования в служебных целях.

Функционирование электронной почты обеспечивается оборудованием, каналами связи и иными ресурсами, принадлежащими Центру. Все почтовые сообщения, переданные или принятые с использованием корпоративной электронной почты, принадлежат Центру и являются неотъемлемой частью его производственного процесса.

Любые сообщения корпоративной электронной почты могут быть прочитаны, использованы в интересах Центра либо удалены уполномоченными сотрудниками Центра.

Сотрудникам Центра запрещено вести частную переписку с использованием средств корпоративной электронной почты Центра. К частной переписке относится переписка, не связанная с исполнением сотрудником своих должностных обязанностей.

Использование корпоративной электронной почты Центра для частной переписки сотрудником, надлежащим образом, ознакомленным с данной Политикой, является нарушением трудовой дисциплины Центра. Подписываясь в ознакомлении с настоящей Политикой, сотрудник даёт согласие на ознакомление и иное использование в интересах Центра его переписки, осуществляемой с использованием корпоративной электронной почты, и соглашается с тем, что любое использование его переписки, осуществляемой с использованием корпоративной электронной почты, не может рассматриваться как нарушение тайны связи.

Каждый сотрудник Центра имеет право на просмотр либо иное использование в интересах Центра сообщений корпоративной электронной почты, которые направлены или получены им, соответственно, с его или на его корпоративный электронный адрес.

Использование сообщений корпоративной электронной почты в интересах Центра, в том числе ознакомление с содержанием сообщений, осуществляется в соответствии с правами доступа к информации, установленными внутренними ОРД о конфиденциальной информации и иными правовыми актами, регламентирующими порядок обращения с информацией ограниченного доступа.

Исходящие электронные сообщения сотрудников Центра должны содержать следующие поля:

- адрес получателя;
- тема электронного сообщения;
- текст электронного сообщения (вложенные файлы);
- подпись отправителя;
- предупреждение о служебном характере сообщения и его конфиденциальности.

Формат подписи отправителя:

С уважением,
<Фамилия имя>
<Должность>
<Структурное подразделение>
<Наименование Учреждения>
<Адрес>
<номера контактов: телефон, мессенджеры, адреса электронной почты>
<сайт>

Формат предупреждения о служебном характере сообщения и его конфиденциальности:

«Это электронное сообщение и любые документы, приложенные к нему, содержат конфиденциальную информацию. Настоящим уведомляем Вас о том, что если это сообщение не предназначено Вам, использование, копирование, распространение информации, содержащейся в настоящем сообщении, а также осуществление любых действий на основе этой информации, строго запрещено и защищается законодательством Российской Федерации. Если Вы получили это сообщение по ошибке, пожалуйста, сообщите об этом отправителю по электронной почте и удалите это сообщение. CONFIDENTIALITY NOTICE: This email and any files attached to it are confidential. If you are not the intended recipient you are notified that using, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited and protected by the laws of the Russian Federation. If you have received this email in error please notify the sender and delete this email.»

При формировании ответов на полученные электронные сообщения можно использовать следующую упрощённую подпись:

С уважением,

<Фамилия имя>

<Номера телефонов, мессенджеры, адреса электронной почты>

В случае получения служебного сообщения о невозможности доставки сообщения адресату или получения извещения от адресата о том, что он не получил отправленное ему сообщение, необходимо связаться с сотрудником отдела ИТ.

Отказ от дальнейшего предоставления сотруднику Центра услуг электронной почты может быть вызван нарушениями требований настоящей Политики.

Прекращение предоставления сотруднику Центра услуг электронной почты наступает при прекращении действия трудового договора (контракта) сотрудника.

8.7.4. Работа в сети интернет

Доступ к сети Интернет предоставляется сотрудникам Центра в целях выполнения ими своих служебных обязанностей, требующих непосредственного подключения к внешним информационным ресурсам.

При использовании сети Интернет необходимо:

• соблюдать требования настоящей Политики;

• использовать сеть Интернет исключительно для выполнения своих служебных обязанностей;

• ставить в известность отдел ИТ о любых фактах нарушения требований настоящей Политики;

При использовании сети Интернет запрещено:

• использовать предоставленный Центром доступ в сеть Интернет в личных целях;

• использовать несанкционированные аппаратные и программные средства, позволяющие получить несанкционированный доступ к сети Интернет;

• совершать любые действия, направленные на нарушение нормального функционирования ИС Центра;

• публиковать, загружать и распространять материалы, содержащие:

- конфиденциальную информацию, за исключением случаев, когда это входит в должностные обязанности и способ передачи является безопасным, согласованным с отделом ИТ;

- угрожающую, клеветническую, непристойную информацию;

- вредоносное ПО, предназначенное для нарушения, уничтожения либо ограничения функциональности любых аппаратных и программных средств, для осуществления несанкционированного доступа, а также ссылки на него;

- фальсифицировать свой IP- адрес, а также прочую служебную информацию.

Общество оставляет за собой право блокировать или ограничивать доступ пользователей к сети Интернет, содержание которых не имеет отношения к исполнению служебных обязанностей, а также к ресурсам, содержание и направленность которых запрещены законодательством.

Информация о посещаемых сотрудниками Центра сети Интернет-ресурсах должна протоколироваться для последующего анализа и, при необходимости, может быть представлена руководителям структурных подразделений для контроля.

Файлы, загружаемые из сети Интернет, подлежат обязательной проверке на отсутствие вредоносного ПО.

8.7.5. Использование мобильных устройств

Под использованием мобильных устройств и носителей информации в ИС Центра понимается их подключение к инфраструктуре ИС с целью обработки, приёма/передачи информации между ИС и мобильными устройствами, а также носителями информации.

На предоставленных Центром мобильных устройствах допускается использование разрешённого в Центре ПО.

К предоставленным Центром мобильным устройствам и носителям информации предъявляются те же требования ИБ, что и для стационарных АРМ. Целесообразность дополнительных мер обеспечения ИБ определяется отделом ИТ.

При использовании предоставленных Центром мобильных устройств и носителей информации, сотрудник обязан:

- соблюдать требования настоящей Политики;
- использовать мобильные устройства и носители информации исключительно для выполнения своих служебных обязанностей;
- ставить в известность отдел ИТ о любых фактах нарушения требований настоящей Политики;
- эксплуатировать и транспортировать мобильные устройства и носители информации в соответствии с требованиями производителей;
- обеспечивать физическую безопасность мобильных устройств и носителей информации всеми разумными способами;
- извещать отдел ИТ о фактах утраты (кражи) мобильных устройств и носителей информации.

При использовании предоставленных сотрудникам Центра мобильных устройств и носителей информации запрещено:

- использовать мобильные устройства и носители информации в личных целях;
- передавать мобильные устройства и носители информации другим лицам (за исключением администраторов ИС и ИБ);
- оставлять мобильные устройства и носители информации без присмотра, если не предприняты действия по обеспечению их физической безопасности.

Любое взаимодействие (обработка, приём\передача информации) инициированное сотрудником Центра между ИС и неучтёнными (личными) мобильным и устройствами, а также носителями информации, рассматривается как несанкционированное (за исключением случаев, оговорённых с администраторами ИС заранее). Руководство Центра оставляет за собой право блокировать или ограничивать использование таких устройств и носителей информации.

Информация об использовании сотрудниками Центра мобильных устройств и носителей информации в ИС должна протоколироваться и, при необходимости, может быть представлена руководителям структурных подразделений, а также руководству Центра.

Информация, хранящаяся на предоставляемых Центром мобильных устройствах и носителях информации, подлежит обязательной проверке на отсутствие вредоносного ПО.

В случае увольнения, предоставленные ему мобильные устройства и носители информации у сотрудника изымаются.

8.7.6. Защита от вредоносного ПО

Отдел ИТ защищает сетевые ресурсы и ИС Центра техническими и программно-аппаратными средствами защиты информации.

При возникновении подозрения на компьютерную атаку (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление о системных ошибках, увеличение исходящего/входящего трафика и т.п.) сотрудник Центра, обнаруживший это, должен незамедлительно оповестить об этом отдел ИТ. После чего администратор ИБ должен заблокировать АРМ, при необходимости передать сведения о компьютерном инциденте в Национальный

координационный центр по компьютерным инцидентам (далее - НКЦКИ) и в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (далее - ГосСопка) провести расследование компьютерного инцидента и составить акт.

Для предупреждения компьютерной атаки рекомендуется:

Всем пользователям:

- никогда не открывать письма, архивы и исполняемые файлы с расширением «exe», полученные в почтовых сообщениях от неизвестного или подозрительного отправителя. Удалять подозрительные вложения, не открывая их, и очищать корзину, где хранятся удаленные сообщения;

- не открывать и не загружать почтовые вложения писем с тематикой, не относящейся к деятельности Центра.

- осуществлять работу с электронной почтой под учетными записями пользователей операционной системы с минимальными возможными привилегиями;

- никогда не загружать файлы и ПО без согласования с отделом ИТ;

Сотрудникам ИТ:

- периодически резервировать важные данные и системную конфигурацию всех информационных систем Центра и хранить резервные копии в безопасном месте;

- Производить проверку почтовых вложений с использованием средств антивирусной защиты Kaspersky Endpoint Security использовав функцию «Защита от почтовых угроз».

8.8. Приобретение, разработка и обслуживание систем

8.8.1 Требования безопасности для информационных систем

При описании требований к созданию новых систем или к усовершенствованию существующих необходимо учитывать потребность в средствах обеспечения безопасности. Требования к безопасности и средства защиты должны соответствовать ценности используемых ИС и потенциальному ущербу для Центра в случае сбоя или нарушения безопасности. Основой для анализа требований к безопасности и выбору мер для поддержки безопасности является оценка рисков и управление рисками. Системные требования к ИБ и процессам, обеспечивающим защиту информации, должны быть включены на ранних стадиях проектирования ИС.

8.8.2 Криптографические средства

Все, полученные Центром, СКЗИ должны быть учтены в соответствующем журнале поэкземплярного учёта СКЗИ (Приложение к приказу ФАПСИ РФ от 13 июня 2001 г. № 152 «Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»). Компрометация или потеря криптографических ключей может привести к нарушению конфиденциальности, подлинности и/или целостности информации. Все ключи должны быть защищены от изменения, утери и уничтожения. Кроме того, секретные и закрытые ключи должны быть защищены от несанкционированного раскрытия. Оборудование, используемое для генерации, хранения и архивирования ключей должно быть физически защищено.

Соглашения с внешними поставщиками криптографических услуг (например, удостоверяющими центрами) об уровне предоставляемого сервиса должны охватывать вопросы ответственности, надёжности сервиса и времени реакции при предоставлении сервиса. Криптографические системы и методы следует использовать для защиты

конфиденциальной информации, когда другие средства контроля не обеспечивают адекватной защиты.

Для критической информации должно использоваться шифрование при их хранении в базах данных или передаче по коммерческим или открытым сетям, таким как Интернет. Шифрование любой другой информации в ИС Центра должно осуществляться только после получения письменного разрешения на это.

8.8.3 Требования по обеспечению ИБ при использовании СКЗИ

СКЗИ должны поставляться разработчиками с полным комплектом эксплуатационной документации, включающей описание ключевой системы, правила работы с ней и обоснование необходимого организационно-штатного обеспечения.

Порядок применения СКЗИ определяется руководством Центра и должен включать:

- порядок ввода в действие, включая процедуры встраивания СКЗИ в ИС;
- порядок эксплуатации;
- порядок восстановления работоспособности в аварийных случаях;
- порядок внесения изменений;
- порядок снятия с эксплуатации;
- порядок управления ключевой информацией;
- порядок обращения с ключевой информацией, включая действия при смене и компрометации ключей.

Для шифрования конфиденциальной информации минимально допустимой длиной ключа является 128 бит.

При использовании шифрования в ИС Центра должны применяться только сертифицированные ФСБ России СКЗИ.

8.8.4 Электронные подписи

ЭП обеспечивает аутентификацию личности, подписавшей электронный документ. ЭП могут применяться для любой формы документа, обрабатываемого электронным способом, при использовании криптографического метода, основывающегося на связанной паре ключей, где один ключ используется для создания подписи (закрытый ключ), а другой – для проверки подписи (открытый ключ).

Необходимо с особой тщательностью обеспечивать конфиденциальность закрытого ключа ЭП, который следует хранить в строжайшем секрете.

Криптографические ключи, используемые для ЭП, должны отличаться от тех, которые используются для шифрования.

8.8.5 Внедрение прикладного программного обеспечения и безопасность информационных систем.

Чтобы свести к минимуму риск повреждения ИС, необходимо обеспечить контроль над внедрением ПО в информационных системах.

Тестирование ПО должно проходить на специальном тестовом стенде, максимально приближенном к рабочей системе по своей архитектуре и содержимому. Тестовые данные, расположенные на стенде, должны находиться под контролем и защитой. Необходимо избегать использования рабочих баз данных, содержащих конфиденциальную информацию на тестовых стендах.

8.8.6 Безопасность процесса обслуживания ИС

Чтобы свести к минимуму вероятность нанесения вреда ИС Центра, следует ввести строгий контроль над внесением изменений в их состав и конфигурацию. Разработаны правила внесения изменений в состав ПО и конфигурацию ИС. Эти правила гарантируют, что процедуры, связанные с безопасностью ИС, не будут нарушены, специалисты технической поддержки, получат доступ только к тем частям системы, которые необходимы для их работы. Для выполнения любого изменения в ИС требуется согласование с начальником отдела ИТ.

После внесения изменений в ИС работа важных для бизнес-процессов Центра приложений должна контролироваться и анализироваться, чтобы гарантировать отсутствие вредных последствий для безопасности ИС Центра.

8.9. Управление инцидентами ИБ

В Центре должна быть разработана и утверждена процедура уведомления о происшествиях в области ИБ, а также процедура реагирования на такие происшествия, включающая в себя действия, которые должны выполняться при поступлении сообщений о происшествии.

Все сотрудники должны быть ознакомлены с процедурой уведомления, а в их обязанности должна входить максимально быстрая передача информации о происшествиях.

В дополнение к уведомлению о происшествиях ИБ и недостатках безопасности должен использоваться мониторинг систем, сообщений и уязвимостей для обнаружения инцидентов ИБ.

Цели управления инцидентами ИБ должны быть согласованы с руководством для учёта приоритетов Центра при обращении с инцидентами.

Необходимо создать механизмы, позволяющие оценивать и отслеживать типы инцидентов, их масштаб и связанные с ними затраты.

8.10. Управление непрерывностью и восстановлением

Центр контролирует процесс обеспечения и поддержки непрерывности бизнес-процессов.

Центр разрабатывает и внедряет необходимые меры, которые позволяют продолжить или восстановить важные бизнес-процессы в установленные сроки после прерывания или сбоя в ИС и обеспечивают требуемый уровень целостности и доступности информации.

Каждая мера поддержки непрерывности бизнеса должна чётко указывать условия начала ее применения и сотрудники, ответственные за реализацию этой меры, включающий в себя:

- алгоритм действий в нештатных ситуациях (алгоритм аварийного восстановления ИС);
- алгоритм действий при возобновлении деятельности бизнес-процессов после аварийного восстановления ИС.

8.11. Соблюдение требований законодательства

Все значимые требования, установленные действующим законодательством, подзаконными актами и договорными отношениями, а также подход Центра к обеспечению соответствия этим требованиям должны быть явным образом определены, документированы и поддерживаться в актуальном состоянии.

Необходимо соблюдение регламентированного процесса, предупреждающего нарушение целостности, достоверности и конфиденциальности информации в ИС, содержащих персональные данные, начиная от стадии сбора, хранения и последующего уничтожения. Персональные данные конкретного сотрудника и процесс их обработки должен быть открытым для этого сотрудника.

В Центре должны быть внедрены соответствующие процедуры для обеспечения соблюдения законодательных ограничений, подзаконных актов и контрактных обязательств по использованию материалов, охраняемых авторским правом, а также по использованию лицензионного ПО.

Важная документация Центра должна быть защищена от утери, уничтожения и фальсификации в соответствии с требованиями законодательства и других подзаконных актов.

8.12. Аудит информационной безопасности

В Центре должны проводиться внутренние проверки СУИБ через запланированные интервалы времени.

Основные цели проведения таких проверок:

- оценка текущего уровня защищённости ИС;
- выявление и локализация уязвимостей в системе защиты ИС;
- анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении ИС;
- оценка соответствия ИС требованиям настоящей Политики;
- выработка рекомендаций по совершенствованию СУИБ за счёт внедрения новых мер защиты информации и повышения эффективности существующих.

В число задач, решаемых при проведении проверок и аудитов СУИБ, входят:

- сбор и анализ исходных данных об организационной и функциональной структуре ИС, необходимых для оценки состояния ИБ;
- анализ существующей Политики и других организационно-распорядительных документов по защите информации на предмет их полноты и эффективности, а также формирование рекомендаций по их разработке (или доработке);
- технико-экономическое обоснование механизмов безопасности;
- проверка правильности подбора и настройки средств защиты информации, формирование предложений по использованию существующих и установке дополнительных средств защиты для повышения уровня надёжности и безопасности ИС;
- разбор инцидентов ИБ и минимизация возможного ущерба от их проявления.

Руководство и сотрудники Центра при проведении у них аудита СУИБ обязаны оказывать содействие аудиторам и предоставлять всю необходимую для проведения аудита информацию.

9. Ответственность

Директор Центра определяет приоритетные направления деятельности в области обеспечения ИБ, меры по реализации настоящей Политики, утверждает списки объектов и сведений, подлежащих защите.

Заместитель директора по административной работе и безопасности осуществляет руководство обеспечением информационной безопасности Центра.

Ответственность за поддержание положений настоящей Политики в актуальном состоянии, создание, внедрение, координацию и внесение изменений в процессы СУИБ Центра лежит на начальнике отдела информационных технологий.

Все руководители несут прямую ответственность за реализацию Политики и её соблюдение персоналом в соответствующих подразделениях.

Сотрудники Центра несут персональную ответственность за соблюдение требований документов СУИБ и обязаны сообщать обо всех выявленных нарушениях в области ИБ в отдел ИТ.

В трудовых договорах и должностных инструкциях работников устанавливается ответственность за сохранность служебной информации, ставшей известной в силу выполнения своих обязанностей.

Руководство Центра регулярно проводит совещания, посвящённые проблемам обеспечения ИБ с целью формирования чётких указаний по этому вопросу, осуществления контроля их выполнения, а также оказания административной поддержки инициативам по обеспечению ИБ.

Нарушение требований организационно – распорядительной документации Центра по обеспечению ИБ является чрезвычайным происшествием и будет служить поводом и основанием для проведения служебного расследования.

10. Контроль и пересмотр

Контроль состояния ИБ Центра осуществляется заместителем директора по административной работе и безопасности.

Текущий контроль соблюдения настоящей Политики осуществляет начальник отдела ИТ и специалист по защите информации. Контроль осуществляется путем проведения мониторинга и менеджмента инцидентов ИБ Центра, по результатам оценки ИБ, а также в рамках иных контрольных мероприятий.

Специалист по защите информации отдела ИТ ежегодно пересматривает положения настоящей Политики. Изменения и дополнения вносятся по инициативе отдела ИТ.

Порядок пересмотра документов второго и третьего уровней определяется в данных документах.

Все изменения, внесённые в настоящую Политику, должны учитываться в листе «Список изменений».

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ п/п	Основание для изменений (дата, № документа)	Номера листов			Дата внесения изменений	Дата введения изменений в действие	Всего листов в документе	Фамилия лица, ответственного за внесение изменений
		Измененных	Новых	Аннулированных				

Лист ознакомления с документом
"Политика информационной безопасности ФГБУ
«НМИЦ детской травматологии и ортопедии имени Г.И. Турнера» Минздрава России"
(утверждено Директором «__» ______ 2025__ г. № _____)

№ п/п	ФИО	Должность	Подпись, дата