Политика

информационной безопасности

Общие положения

1) Политика информационной безопасности (далее Политика) ОГБУЗ Городская Больница города Костромы (далее - Организация) представляет собой систематизированное изложение целей, задач и принципов защиты в области информационной безопасности, которыми руководствуется Организация в своей деятельности. Кроме того Политика информационной безопасности закрепляет неотвратимость и обязательность ответственности за нарушения положений организации в области защиты информации.
2) Политика учитывает современное состояние и ближайшие перспективы развития информационных технологий и их безопасности в Организации.
3) Использование данной Политики в качестве основы для построения комплексной системы информационной безопасности Организации позволит оптимизировать затраты на ее построение.
4) Основные положения и требования данного документа распространяются на все структурные подразделения Организации. Политика информационной безопасности распространяется на физические и юридические лица, взаимодействующие с Организацией в качестве поставщиков и потребителей информационных ресурсов Организации в том или ином качестве.
5) Законодательной основой настоящей Политики являются Конституция Российской Федерации, Гражданский и Уголовный кодексы, законы, указы, постановления, и другие нормативные документы действующего законодательства Российской Федерации.
6) Политика является методологической основой для:

- Формирования и функционирования единой системы в области обеспечения безопасности информации Организации;
- Принятия управленческих решений и разработке практических мер по воплощению политики безопасности информации и выработки комплекса согласованных мер, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз безопасности информации;
- Координации деятельности структурных подразделений Организации при проведении работ по созданию, развитию и эксплуатации информационных систем с соблюдением требований по обеспечению безопасности информации;
- Разработки предложений по совершенствованию правового, нормативного, технического и организационного обеспечения безопасности информации в Организации.
- Составления комплекта документации в области защиты информации Организации, куда могут входить инструкции, положения и руководства.
- Комплект документов в области защиты информации Организации, который будет приниматься и дополняться в целях раскрытия и уточнения положений данной Политики, должен быть с ней согласован и не противоречить ей.

Объекты

1) Объектами безопасности являются:

- персонал (руководство, ответственные исполнители, сотрудники);
- финансовые средства, материальные ценности, новейшие технологии;
- информационные ресурсы (информация с ограниченным доступом, составляющая коммерческую тайну, иная конфиденциальная информация, предоставленная в виде документов и массивов независимо от формы и вида их представления)

2) Все объекты подлежат защите по нормам действующего законодательства и непротиворечащим ему локальным актам Организации.

Термины

1) Основные термины и определения, которые будут использоваться в документации по защите информации и информационных технологий

- **Информация** - сведения о предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;
- **Информационные ресурсы** - отдельные документы и отдельные массивы;
- **Конфиденциальность информации** - субъективно определяемая (приписываемая) информации характеристика (свойство), указывающая на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемая способностью системы (среды) сохранять указанную информацию в тайне от субъектов, не имеющих полномочий на право доступа к ней;
- **Доступность информации** - важнейшее свойство системы, в которой циркулирует информация (средств и технологии ее обработки), характеризующееся способностью обеспечивать своевременный беспрепятственный доступ к информации субъектов, имеющих на это надлежащие полномочия;
- **Целостность информации** - свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию);
- **Доступ к информации** - ознакомление с информацией или получение возможности ее обработки. Доступ к информации регламентируется ее правовым режимом и должен сопровождаться строгим соблюдением его требований. Доступ к информации, осуществленный с нарушениями требований ее правового режима, рассматривается как несанкционированный доступ;
- **Автоматизированная система обработки информации** - организационно-техническая система, представляющая собой совокупность следующих взаимосвязанных компонентов: технических средств обработки и передачи данных, методов и алгоритмов обработки в виде соответствующего программного обеспечения, массивов данных на различных носителях, персонала и пользователей, объединенных для выполнения автоматизированной обработки данных;
- **Уязвимость автоматизированной системы** - любая характеристика автоматизированной системы, использование которой может привести к реализации угрозы;
- **Безопасность информации** - защищенность информации от нежелательного (для соответствующих субъектов информационных отношений) ее разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности информации, а также незаконного ее тиражирования;
- **Система информационной безопасности** - совокупность (комплекс) специальных мер правового (законодательного) и административного характера, организационных мероприятий, физических и технических (программных и аппаратных) средств защиты, а также специального персонала, предназначенных для обеспечения информационной безопасности Организации;
- **Защита информации** - деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на информацию;
- **Объект защиты** - информация или носитель информации или информационный процесс, в отношении которых необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации;

- **Средство защиты информации** - техническое, программное средство, вещество и/или материал, предназначенные или используемые для защиты информации;
- **Администратор безопасности** - лицо, ответственное за обеспечение безопасности системы, за реализацию и непрерывность соблюдения установленных административных мер защиты и осуществляющих постоянную организационную поддержку функционирования применяемых физических и технических средств защиты;
- **Пользователь** - субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации;
- **Угроза** - реально или потенциально возможные действия по реализации опасных воздействующих факторов с целью преднамеренного или случайного (неумышленного) нарушения режима функционирования объекта и нарушения свойств защищаемой информации или других ресурсов объекта;
- **Злоумышленник** - нарушитель, действующий намеренно из корыстных, идейных или иных побуждений;
- **Нарушитель** - это лицо (субъект), которое предприняло (пыталось предпринять) попытку несанкционированного доступа к ресурсам системы (попытку выполнения запрещенных ему действий с данным ресурсом) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или с целью самоутверждения и т.п.) и использовавшее для этого различные возможности, методы и средства;
- **Атака на информационную систему** - любое действие, выполняемое нарушителем, которое приводит к реализации угрозы, путем использования уязвимостей системы,
- **Вредоносные программы** - программы или измененные программы объекта информатизации, приводящие к несанкционированному уничтожению, блокированию, модификации либо копированию информации или нарушению работы.

3) В документации по защите информации могут быть использование иные термины, которые будут закреплены непосредственно в этих документах или в актах, на которые ссылаются эти документы.

Принципы реализации политики

При достижении поставленных целей и реализации задач, Организация руководствоваться следующими принципами:

- **Законность** - Предполагает осуществление защитных мероприятий и разработку системы безопасности информации Организации в соответствии с действующим законодательством в области информации, информатизации и защиты информации, а также других нормативных актов по безопасности информации, утвержденных органами государственной власти и управления в пределах их компетенции, с применением всех дозволенных методов обнаружения и пресечения правонарушений при работе с информацией. Принятые меры безопасности информации не должны препятствовать доступу правоохранительных органов в предусмотренных законодательством случаях к информации конкретных подсистем. Все пользователи информационной системы Организации должны иметь представление об ответственности за правонарушения в области информации.
- **Системность** - Системный подход к построению системы защиты информации в Организации предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности информации Организации. При создании системы защиты должны учитываться все слабые и наиболее уязвимые места информационной системы Организации, а также возможные объекты направления атак со

стороны нарушителей, пути проникновения в распределенные системы и несанкционированного доступа к информации. Система защиты должна строиться с учетом не только всех известных каналов проникновения и несанкционированного доступа к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

- **Комплексность** - Комплексное использование методов и средств защиты компьютерных систем предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов. Защита должна строиться эшелонировано. Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами.
- **Непрерывность** - Обеспечение безопасности информации — это не только и процедура или политика, которая осуществляется в определенный отрезок времени или совокупность средств защиты, это процесс, который должен постоянно идти на всех уровнях внутри Организации, и каждый сотрудник Организации должен принимать участие в этом процессе.
- **Своевременность** - Предполагает упреждающий характер мер обеспечения безопасности информации, то есть постановку задач по комплексной защите информации и реализацию мер обеспечения безопасности информации на ранних стадиях разработки информационных систем в целом и их систем защиты информации, в частности. Разработка системы защиты должна вестись параллельно с разработкой и развитием самой защищаемой информационной системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, создать более эффективные системы, обладающие достаточным уровнем защищенности.
- **Преемственность и непрерывность совершенствования** - Предполагает постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования информационной системы Организации и системы ее защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.
- **Персональная ответственность** - Предполагает возложение ответственности за обеспечение безопасности информации и системы ее 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 виновников был четко известен или сведен к минимуму.
- **Минимизация полномочий** - Означает предоставление пользователям минимальных прав доступа в соответствии со служебной необходимостью. Доступ к информации должен предоставляться только в том случае и объеме, если это необходимо сотруднику для выполнения его должностных обязанностей.
- **Гибкость системы защиты** - Система обеспечения информационной безопасности должна быть способна реагировать на изменения внешней среды и условий осуществления Организации своей деятельности. Свойство гибкости системы обеспечения информационной безопасности необходимости принятия кардинальных мер по полной замене средств и методов защиты на новые.
- **Обоснованность и техническая реализуемость** - Информационные технологии, технические и программные средства, средства и меры защиты информации должны быть реализованы на современном уровне развития науки и техники, обоснованы с точки зрения достижения заданного уровня безопасности информации и экономической целесообразности, а также должны соответствовать установленным нормам и требованиям по безопасности информации.
- **Обязательность контроля** - Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил, обеспечения безопасности

информации, на основе используемых систем и средств защиты информации, при совершенствовании критериев и методов оценки эффективности этих систем и средств. Контроль, за деятельностью любого пользователя, каждого средства защиты и в отношении любого объекта защиты должен осуществляться на основе применения средств оперативного контроля и регистрации и должен охватывать как несанкционированные, так и санкционированные действия пользователей.

Цели Политики

Целями настоящей Политики являются:

- Сохранение конфиденциальности критичных информационных ресурсов;
- Полное соответствие требованиям законодательства РФ в части информационной безопасности;
- Обеспечение целостности информации
- Достижение полной осведомленности пользователей в области рисков, связанных с информационными ресурсами Организации;
- Предотвращение и (или) максимальное снижение ущерба от реализации угроз информационной безопасности;
- Определение степени ответственности и обязанностей сотрудников по обеспечению информационной безопасности в Организации;
- Обеспечение непрерывности доступа к информационным ресурсам Организации;
- Достижение продуктивности мер по защите от угроз информационных систем;
- Достижение максимальной автономности работы системы информационной безопасности организации.

Основные задачи системы обеспечения безопасности информации

Для достижения целей защиты информации система обеспечения информационной безопасности должна обеспечивать эффективное решение следующих задач:

- Своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба заинтересованным субъектам информационных отношений, нарушению нормального функционирования информационных систем Организации;
- Создание механизма оперативного реагирования на угрозы безопасности информации и негативные тенденции;
- Создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации;
- Организация защиты от вмешательства в процесс функционирования информационных систем Организации посторонних лиц;
- Обеспечение стабильного функционирования криптографических средств защиты информации;
- Обеспечение аутентификации пользователей, участвующих в информационном обмене (подтверждение подлинности отправителя и получателя информации);
- Обеспечение защиты от несанкционированной модификации используемых в корпоративной информационной системе Организации программных средств, а также защиту системы от внедрения несанкционированных программ, включая компьютерные вирусы;
- Обеспечение защиты информации ограниченного пользования от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи;

- Выполнение действующих, а также всех последующих требований законодательства в области защиты информации;
- Разграничение доступа пользователей к информационным, аппаратным, программным и иным ресурсам Организации.

Ответственность за нарушения положений Политики информационной безопасности и дополняющего ее комплекта документов

1) Любое грубое нарушение порядка и правил пользования информационными ресурсами Организации должно расследоваться. К виновным должны применяться адекватные меры воздействия.
2) Мера ответственности персонала за действия, совершенные в нарушение установленных правил обеспечения безопасной работы с информацией, должна определяться нанесенным ущербом, наличием злого умысла и другими факторами по усмотрению руководства Организации.
3) В случае если нарушение выходит за рамки дисциплинарного взыскания могут привлекаться органы правопорядка для оказания содействия.

Порядок утверждения, внесения изменений и дополнений, ознакомления

1) Настоящая Политика вступает в законную силу с даты утверждения руководителя Организации (главного врача). Внесение Изменений и дополнений в настоящую Политику рассматривается по инициативе администратора безопасности, руководителя Организации и начальника отдела автоматизированных систем управления Организации.
2) В случае вступления отдельных пунктов Политики или положений документации по защите информации в противоречие с новыми законодательными актами, эти пункты и положения утрачивают юридическую силу до момента внесения изменений в настоящую Политику или документацию по информационной безопасности.
3) Положения Политики и документации по информационной безопасности сотрудникам Организации разъясняет администратор безопасности, фактом подтверждения того, что сотрудник ознакомлен и не имеет вопросов на момент ознакомления является его подпись в журнале «Инструктажа сотрудников ОГБУЗ ГБ г. Костромы по Информационной безопасности»