УТВЕРЖДЕНО

Приказ УЗ «Могилевский облЦГЭиОЗ»

от 13.05.2025 № 75

Политика информационной безопасности

в ЦГЭ Могилевской области

ГЛАВА 1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Политика разработана в соответствии с законодательством Республики Беларусь, регулирующим вопросы обеспечения информационной безопасности.

1. Настоящая Политика является документом, доступным любому работнику в учреждениях, осуществляющих государственный санитарный надзор, Могилевской области (далее – ЦГЭ области) и пользователю их ресурсов, и представляет собой официально принятую систему взглядов на проблему обеспечения информационной безопасности, устанавливает принципы построения системы управления информационной безопасностью на основе систематизированного изложения целей, процессов и процедур информационной безопасности ЦГЭ области.
2. Руководители ЦГЭ области осознают важность и необходимость развития и совершенствования мер и средств обеспечения информационной безопасности. Соблюдение требований информационной безопасности позволит упорядочить информационные процессы ЦГЭ области, привести к соответствию правовым нормам, улучшить имидж и деловую репутацию.
3. Требования информационной безопасности, которые предъявляются ЦГЭ области, соответствуют политике и функциям ЦГЭ области и предназначены для снижения рисков, связанных с информационной безопасностью.
4. Стратегия ЦГЭ области в области обеспечения информационной безопасности и защиты информации наряду с прочим включает выполнение в практической деятельности законодательства Республики Беларусь в области безопасности, безопасности информационных технологий и защиты информации, безопасности персональных данных.

1.6. Необходимые требования обеспечения информационной безопасности ЦГЭ области должны неукоснительно соблюдаться их работниками.

1.7. Работники ЦГЭ области, не ознакомленные с настоящей Политикой, не допускаются к работе с информационными системами и ресурсами ЦГЭ области.

1.8. Настоящая Политика распространяется на все информационные процессы ЦГЭ области и обязательна для применения всеми работниками ЦГЭ области, а также пользователями их информационных ресурсов.

1.9. Дополнительно к данной Политике могут быть при необходимости разработаны отдельные документы, детализирующие ее положения применительно к одной или нескольким информационным системам, видам и технологиям деятельности ЦГЭ области.

ГЛАВА 2. СПИСОК ТЕРМИНОВ И ОПРЕДЕЛЕНИЙ

1. Информационные процессы – последовательность технологически связанных операций по поиску, хранению, передаче, обработке и использованию информации, необходимых для обеспечения деятельности ЦГЭ области.
2. Информационная безопасность (далее − ИБ) в настоящей Политике − состояние защищенности информационных активов ЦГЭ области от угроз, способных нарушить их конфиденциальность, целостность или доступность.
3. Информационная система − совокупность программно-аппаратных комплексов конкретных ЦГЭ области, применяемых для обеспечения их информационных процессов.
4. Инцидент информационной безопасности − это появление одного или нескольких нежелательных рисковых событий информационной безопасности, с которыми связана значительная вероятность нарушения конфиденциальности, целостности или доступности информационных активов и инфраструктуры и создания угрозы информационной безопасности.

2.5. Конфиденциальная информация (далее − КИ) − информация, в отношении которой ЦГЭ области и законодательством Республики Беларусь установлен режим конфиденциальности.

2.6. Модель угроз − описательное представление свойств или характеристик угроз безопасности информации.

1. Модель нарушителя − описательное представление опыта, знаний, доступных ресурсов возможных нарушителей ИБ, необходимых им для реализации угрозы ИБ, и возможной мотивации действий.
2. Ответственное подразделение − отдел ОКиАСУ УЗ «Могилевский облЦГЭиОЗ». Основные функции ответственного подразделения − внедрение настоящей Политики, разработка, внедрение и поддержка систем обеспечения информационной безопасности в ЦГЭ области.

2.9. Пользователь информационной системы − физическое лицо, обладающее возможностью доступа к информационной системе в ЦГЭ области.

2.10. Режим конфиденциальности информации − организационно- технические мероприятия по защите информации, позволяющие обладателю КИ при любых обстоятельствах обеспечить её сохранность и конфиденциальность, включающие в себя:

1. установление перечня КИ (прим.: определяется в ***Приложении 1*** к настоящей Политике);
2. ограничение доступа к КИ путем установления порядка обращения с этой информацией и контроля над соблюдением такого порядка;

2.10.3. регулирование отношений по использованию КИ работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров и соглашений.

1. Рисковое событие информационной безопасности − это событие, повлекшее или способное повлечь за собой репутационные и финансовые потери ЦГЭ области и произошедшее по причине ошибочности или сбоя процессов, действий людей и систем, а также по причине внешних событий.
2. Угроза информационной безопасности − любой риск, влияющий на нарушение одного (или нескольких) свойств информации: целостности, конфиденциальности, доступности объектов защиты.

ГЛАВА 3. ОПИСАНИЕ ОБЪЕКТА ЗАЩИТЫ

3.1. Основными объектами защиты системы информационной безопасности в ЦГЭ области являются:

3.1.1. содержащаяся в информационных ресурсах ЦГЭ области информация, обрабатываемая или хранимая в рамках их деятельности, независимо от формы и вида ее представления, в т.ч. содержащая служебную тайну и конфиденциальная, персональные данные физических лиц, сведения ограниченного распространения, а также открыто распространяемая информация;

1. информационная инфраструктура, включающая системы хранения, обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены такие системы.

ГЛАВА 4. ЦЕЛИ И ЗАДАЧИ ДЕЯТЕЛЬНОСТИ

ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4.1. Целью деятельности по обеспечению информационной безопасности ЦГЭ области является обеспечение защищённости информационных активов ЦГЭ области от актуальных угроз за счёт реализации комплекса организационных и технических мер.

4.2. Основные задачи деятельности по обеспечению информационной безопасности ЦГЭ области:

1. своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба субъектам информационных отношений, нарушению нормального функционирования систем ЦГЭ области;
2. предотвращение инцидентов нарушения информационной безопасности;
3. создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации;
4. защита от вмешательства в процесс функционирования систем ЦГЭ области посторонних лиц (доступ к информационным ресурсам должны иметь только зарегистрированные в установленном порядке пользователи);

4.2.5. разграничение доступа пользователей к информационным, аппаратным, программным и иным ресурсам ЦГЭ области (обеспечение доступа только к тем ресурсам и выполнению только тех операций с ними, которые необходимы конкретным пользователям для выполнения своих служебных обязанностей);

1. обеспечение аутентификации пользователей, имеющих допуск в информационные сети и участвующих в информационном обмене (подтверждение подлинности отправителя и получателя информации);
2. защиту от несанкционированной модификации используемых в системах ЦГЭ области программных средств, а также защиту систем от внедрения несанкционированных программ, включая компьютерные вирусы;
3. защиту информации от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи.

ГЛАВА 5. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

5.1. Под антропогенными угрозами ИБ понимается:

1. угрозы, вызванные ошибками в проектировании информационной системы и ее элементов;
2. ошибки в действиях персонала;
3. умышленные действия, связанные с корыстными, идейными или иными устремлениями людей;
4. угрозы, связанные с нестабильностью и противоречивостью требований регуляторов деятельности ЦГЭ области и контрольных органов;
5. угрозы, связанные с действиями в руководстве и управлении, неадекватными целям и сложившимся условиям, с потребляемыми услугами, с человеческим фактором.

5.2. Под техногенными угрозами ИБ понимается:

5.2.1. угрозы объективных физических процессов техногенного характера;

5.2.2. техническое состояние окружения объекта угрозы или его самого, не обусловленное напрямую деятельностью человека;

5.2.3. сбои в работе или разрушение систем, созданных человеком, находящихся вне зоны ответственности ЦГЭ области.

5.3. Под природными угрозами ИБ понимается:

1. угрозы объективных физических процессов природного характера;
2. стихийных природных явлений;

5.3.3. состояний физической среды, не обусловленных напрямую деятельностью человека;

5.3.4. угрозы метеорологические, атмосферные, геофизические, геомагнитные и прочие, включая экстремальные климатические условия, метеорологические явления, стихийные бедствия.

ГЛАВА 6. МОДЕЛЬ НАРУШИТЕЛЯ

ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

6.1. В качестве потенциальных внутренних нарушителей рассматриваются:

6.1.1. зарегистрированные пользователи информационных систем ЦГЭ области;

6.1.2. работники, не являющиеся зарегистрированными пользователями и не допущенные к ресурсам информационных систем ЦГЭ области, но имеющие доступ в здания и помещения;

6.1.3. персонал, обслуживающий технические средства информационных систем ЦГЭ области;

6.1.4. руководители различных уровней.

6.2. В качестве потенциальных внешних нарушителей рассматриваются:

1. бывшие работники ЦГЭ области;
2. сторонние организации или их представители, задействованные в разработке и сопровождении программного обеспечения и взаимодействующие по вопросам технического обеспечения ЦГЭ области;

6.2.3. сторонние организации или их представители, предоставляющие собственные ресурсы в пользование ЦГЭ области;

1. посетители информационных ресурсов ЦГЭ области;
2. посетители зданий и помещений ЦГЭ области;
3. члены преступных организаций или лица, действующие по их заданию;

6.2.7. лица, случайно или умышленно проникшие в информационные системы ЦГЭ области из внешних телекоммуникационных сетей.

6.3. В отношении внутренних и внешних нарушителей принимаются следующие ограничения и предположения о характере их возможных действий:

6.3.1. нарушитель скрывает свои несанкционированные действия от других работников;

1. несанкционированные действия нарушителя могут быть следствием ошибок пользователей, эксплуатирующего и обслуживающего персонала, а также недостатков принятой технологии обработки, хранения и передачи информации;
2. в своей деятельности вероятный нарушитель может использовать любое имеющееся средство перехвата информации, воздействия на информацию и информационные системы, адекватные финансовые средства для подкупа персонала, шантаж и другие средства и методы для достижения стоящих перед ним целей;
3. внешний нарушитель может действовать в сговоре с внутренним нарушителем.

 6.4. Нарушитель может стремиться к получению несанкционированного доступа, копированию, модификации, удалению или блокировке информации, а также к подрыву доступности или целостности систем.

ГЛАВА 7. ОСНОВНЫЕ ПОЛОЖЕНИЯ

ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

7.1. Требования об обеспечении информационной безопасности ЦГЭ области обязательны к соблюдению всеми работниками и пользователями информационных систем.

7.2. Стратегия ЦГЭ области в части противодействия угрозам ИБ заключается в реализации взаимодополняющих мер по обеспечению безопасности: от организационных мер на уровне руководителей ЦГЭ области до специализированных мер информационной безопасности по каждому выявленному риску или случаю.

7.3. При планировании мероприятий по обеспечению информационной безопасности в ЦГЭ области осуществляются:

7.3.1. Определение и распределение ролей персонала ЦГЭ области, связанного с обеспечением информационной безопасности (ролей информационной безопасности).

1. Управление рисками информационной безопасности.

7.4. В рамках реализации деятельности по обеспечению информационной безопасности в ЦГЭ области осуществляются:

7.4.1. Управление инцидентами информационной безопасности, включающее, но не исключительно:

1. учет всех подлежащих защите информационных систем;
2. сбор информации о событиях информационной безопасности;
3. выявление и анализ инцидентов информационной безопасности;
4. расследование инцидентов информационной безопасности;

7.4.1.5. оперативное реагирование на инцидент информационной безопасности;

7.4.1.6. минимизацию негативных последствий инцидентов информационной безопасности;

7.4.1.7. оперативное доведение до руководителей ЦГЭ области информации о наиболее значимых инцидентах информационной безопасности и оперативное принятие решений по ним, включая регламентирование порядка реагирования на инциденты информационной безопасности;

7.4.1.8. взаимодействие с компетентными органами безопасности по выявленным инцидентам;

1. выполнение принятых решений по всем инцидентам информационной безопасности в установленные сроки;
2. пересмотр применяемых требований, мер и механизмов по обеспечению информационной безопасности по результатам рассмотрения инцидентов информационной безопасности;

7.4.1.11. регулярный контроль уровня знаний персонала ЦГЭ области в вопросах обеспечения информационной безопасности;

7.4.1.12. обеспечение регламентации и управления доступом к программным и программно-техническим средствам и сервисам автоматизированных систем ЦГЭ области и информации, обрабатываемой в них;

1. обеспечение бесперебойной работы автоматизированных систем и сетей связи;
2. обеспечение возобновления работы автоматизированных систем и сетей связи после прерываний и нештатных ситуаций;
3. применение программных и аппаратных средств защиты от вредоносных программ;

7.4.1.16. обеспечение информационной безопасности при использовании доступа в сеть Интернет и услуг электронной почты;

1. подготовка работников, ответственных за организацию и осуществление практических мероприятий по обеспечению информационной безопасности.

7.4.2. Обеспечение защиты информации от утечки по техническим каналам, включающее:

1. применение мер и технических средств, снижающих вероятность несанкционированного получения информации в устной форме − пассивная защита;
2. применение мер и технических средств, создающих помехи при попытке несанкционированного получения информации − активная защита;
3. применение мер и технических средств, позволяющих выявлять каналы несанкционированного получения информации − поиск.

7.5. В целях проверки деятельности по обеспечению информационной
безопасности в ЦГЭ области осуществляются:

7.5.1. контроль правильности реализации и использования мер защиты;

7.5.2. контроль изменений конфигурации систем и подсистем;

7.5.3. мониторинг факторов рисков и соответствующий их пересмотр;

7.5.4. контроль реализации и исполнения требований работниками ЦГЭ области действующих внутренних нормативных документов по обеспечению информационной безопасности;

7.6. В целях совершенствования деятельности по обеспечению информационной безопасности в ЦГЭ области осуществляется периодическое и, при необходимости, оперативное уточнение и пересмотр целей и задач обеспечения информационной безопасности.

ГЛАВА 8. ОРГАНИЗАЦИОННАЯ ОСНОВА ДЕЯТЕЛЬНОСТИ

ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

8.1. В целях выполнения задач по обеспечению информационной безопасности ЦГЭ области, в соответствии с рекомендациями стандартов, принятых в Республике Беларусь и международных стандартов по безопасности, в (для) ЦГЭ области определены следующие роли:

1. Ответственное подразделение – отдел КПРиАСУ областного ЦГЭиОЗ;
2. Ответственный работник – IT-специалист каждого из ЦГЭ области (при наличии).

8.2. При необходимости могут быть определены и другие роли и права к ним по информационной безопасности.

8.3. Оперативная деятельность и планирование деятельности по обеспечению информационной безопасности ЦГЭ области осуществляются и координируются специалистами Ответственного подразделения.

Задачами Ответственного подразделения и ответственных работников являются:

8.3.1. установление потребностей ЦГЭ области в применении мер обеспечения информационной безопасности, определяемых внутренними требованиями и требованиями нормативных актов;

1. соблюдение действующего законодательства, нормативных актов в области обеспечения безопасности и технической защиты информации;
2. разработка и пересмотр внутренних нормативных документов по обеспечению информационной безопасности ЦГЭ области;
3. осуществление контроля актуальности и непротиворечивости внутренних нормативных документов, затрагивающих вопросы информационной безопасности;
4. обучение, контроль и непосредственная работа с персоналом ЦГЭ области в области обеспечения информационной безопасности;
5. планирование применения и эксплуатации средств обеспечения информационной безопасности на объектах и системах в ЦГЭ области;
6. выявление и предотвращение реализации угроз информационной безопасности;

8.3.8. выявление и реагирование на инциденты информационной безопасности;

8.3.9. информирование в установленном порядке администрации (ответственных лиц) об угрозах и рисковых событиях информационной безопасности;

8.3.10. прогнозирование и предупреждение инцидентов информационной безопасности;

8.3.11. пресечение несанкционированных действий нарушителей информационной безопасности;

1. обеспечение эксплуатации средств и механизмов обеспечения информационной безопасности;
2. мониторинг и оценка информационной безопасности, включая оценку полноты и достаточности, защитных мер и видов деятельности по обеспечению информационной безопасности ЦГЭ области;

8.3.14. контроль обеспечения информационной безопасности ЦГЭ области, в том числе, и на основе информации об инцидентах информационной безопасности, результатах мониторинга, оценки и аудита информационной безопасности;

8.3.15. информирование руководителей ЦГЭ области об угрозах информационной безопасности, влияющих на деятельность ЦГЭ области.

8.3.16 следование в своей работе рекомендациям оперативно-аналитического центра при Президенте Республики Беларусь (ОАЦ) по обеспечению безопасности информации в локальных сетях, подключенных к сети Интернет, по обеспечению безопасности информации интернет ресурсов государственных органов (прим.: на основе рекомендаций разработан «Регламент обеспечения безопасности информации в локальной сети, при использовании Интернета, электронной почты и соблюдения правил эксплуатации офисной техники» согласно ***Приложению 2*** к настоящей Политике);

8.3.17 следование в своей работе рекомендациям РНПЦ МТ.

8.4. Финансирование работ по реализации положений настоящей Политики осуществляется в рамках выделяемых средств на информатизацию ЦГЭ области.

8.5. Основными задачами работников ЦГЭ области при выполнении возложенных на них обязанностей и в рамках их участия в оперативной деятельности по обеспечению информационной безопасности ЦГЭ области являются:

8.5.1. осознание персональной ответственности за свои действия в рамках своих функциональных обязанностей при доступе к информационным ресурсам;

8.5.2. соблюдение требований информационной безопасности, устанавливаемых нормативными документами ЦГЭ области;

8.5.3. выявление и предотвращение реализации угроз информационной безопасности в пределах своей компетенции;

8.5.4. выявление и реагирование на инциденты информационной безопасности;

1. информирование в установленном порядке ответственных лиц о выявленных угрозах и рисковых событиях информационной безопасности;
2. прогнозирование и предупреждение инцидентов информационной безопасности в пределах своей компетенции;
3. мониторинг и оценка информационной безопасности в рамках своего участка работы (рабочего места, структурного подразделения) и в пределах своей компетенции;

8.5.8. информирование своего руководства и ответственного подразделения о выявленной угрозе в информационной среде.

ГЛАВА 9. ОТВЕТСТВЕННОСТЬ ЗА СОБЛЮДЕНИЕ

ПОЛОЖЕНИЙ ПОЛИТИКИ

1. Общее руководство обеспечением информационной безопасности ЦГЭ области осуществляет руководитель ответственного подразделения.
2. Ответственность за поддержание положений настоящей Политики в актуальном состоянии, создание, внедрение, координацию и внесение изменений в процессы системы менеджмента информационной безопасности ЦГЭ области лежит на IT-специалистах ответственного подразделения.

9.3. Неисполнение или некачественное исполнение работниками ЦГЭ области обязанностей по обеспечению информационной безопасности может повлечь лишение доступа к информационным системам, а также применение к виновным мер воздействия в рамках действующего законодательства Республики Беларусь.

ГЛАВА 10. КОНТРОЛЬ НАД СОБЛЮДЕНИЕМ

ПОЛОЖЕНИЙ ПОЛИТИКИ

10.1. Общий контроль состояния информационной безопасности в ЦГЭ области осуществляет заместитель главного врача областного ЦГЭиОЗ по хозяйственной работе.

10.2. Текущий контроль соблюдения настоящей Политики осуществляют IT-специалисты ответственного подразделения. Контроль осуществляется путем проведения мониторинга и менеджмента инцидентов информационной безопасности, по результатам оценки информационной безопасности, а также в рамках иных контрольных мероприятий.

ГЛАВА 11. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

1. Требования настоящей Политики могут развиваться другими внутренними нормативными документами ЦГЭ области, которые дополняют и уточняют ее.
2. В случае изменения действующего законодательства и иных нормативных актов, а также Уставов ЦГЭ области настоящая Политика и изменения к ней применяются в части, не противоречащей вновь принятым законодательным и иным нормативным актам, а также Уставам. В этом случае Ответственное подразделение обязано незамедлительно инициировать внесение соответствующих изменений в настоящую Политику и доведение их до всех заинтересованных работников ЦГЭ области.
3. Внесение изменений в настоящую Политику осуществляется на периодической и внеплановой основе:

11.3.1. периодическое определение необходимости изменений в настоящую Политику должно осуществляться каждые 2 года;

11.3.2. внеплановое внесение изменений в настоящую Политику может производиться по результатам анализа инцидентов информационной безопасности, актуальности, достаточности и эффективности используемых мер обеспечения информационной безопасности, по результатам проведения внутренних аудитов информационной безопасности и других контрольных мероприятий.

11.4. Ответственным за внесение изменений в настоящую Политику является руководитель ответственного подразделения.

**Приложение** **1**

к Политике информационной безопасности

в ЦГЭ Могилевской области

**Перечень**

**конфиденциальной информации в ЦГЭ Могилевской области**

1. Информация об основной, хозяйственной и финансовой деятельности ЦГЭ, в том числе:
- материалы надзорной деятельности, административных процессов, административных процедур, рассмотрения обращений, т.д.;

- служебная переписка;

- результаты проверок, в т.ч. внутренних;
- сведения о запланированных и осуществлённых финансовых операциях (счета, платежные поручения, договоры, отчётность), коды доступа к счетам, т.д.;

2. Логины, пароли, ключи доступа, электронные сертификаты, PIN-коды:

- к информационным системам и ресурсам ЦГЭ (вне зависимости от местонахождения);

- к файловым хранилищам, в том числе локальным и облачным;

- к серверному и сетевому оборудованию ЦГЭ;

- к медицинским информационным системам (МИС), государственным информационным системам (ИАС КНД, ЕГБДП и т.д);

- к почтовым, аналитическим, облачным, архивным и иным специализированным сервисам и т.д.

3. Информация о средствах защиты информации, в том числе:

- параметры настройки межсетевых экранов, антивирусного ПО, СЗИ НСД;

- методы резервного копирования и восстановления данных;

- используемые политики доступа и журналирование.

4. Документы, материалы и сведения, отнесённые к конфиденциальной информации внутренними правовыми актами ЦГЭ или содержащие гриф «Секретно» (при наличии) или «Для служебного пользования».

5. Персональные данные работников ЦГЭ, включая:

- анкетные и биографические данные;

- сведения о заработной плате и начислениях;

- кадровые документы (личные дела, трудовые договоры, приказы и пр.);

- данные о медицинских осмотрах, листках нетрудоспособности и т.д.

6. Персональные данные граждан, обрабатываемые в рамках деятельности ЦГЭ, в том числе полученные при обращениях граждан, осуществлении надзора, проведении эпидемиологических расследований, ведении административных процессов, т.п.

7. Сведения, составляющие врачебную тайну, включая:

- информацию о состоянии здоровья пациента;

- диагнозы, результаты обследований и лечения;

- сведения о диспансерном наблюдении и медицинских осмотрах;

- иные данные, позволяющие идентифицировать личность пациента и его медицинское состояние.

**Приложение 2**

к Политике информационной безопасности

в ЦГЭ Могилевской области

Регламент

обеспечения безопасности информации в локальной сети (ЛВС),

при использовании Интернета, электронной почты

и соблюдения правил эксплуатации офисной техники

1. **Права и обязанности пользователей информационных ресурсов (т.е. всех работников ЦГЭ) и администраторов ЛВС (т.е. IT-специалистов)**

**Пользователь** информационных ресурсов **имеет право**:

* на получение надлежащего и исправного АРМ для выполнения непосредственных функциональных обязанностей;
* при невозможности или неэффективности выполнения порученной ему работы имеющимися программно-аппаратными средствами сообщить об этом непосредственному руководителю;
* обращаться к IT-специалистам за консультациями по вопросам функционирования информационных ресурсов;
* получать консультации по работе с компьютерным оборудованием и программным обеспечением общего пользования, по вопросам компьютерной безопасности;
* сменить свой пароль доступа к информационным ресурсам, не используемым совместно с другими работниками, о чем незамедлительно проинформировать IT-специалиста;
* знакомиться с настоящим Регламентом и Политикой информационной безопасности для ЦГЭ области, получать информацию об их изменениях, изменениях правил работы на конкретном оборудовании.

**Руководители структурных подразделений также имеют право** для обеспечения работы возглавляемых структурных подразделений подавать на рассмотрение руководителю ЦГЭ заявки на выделение и модернизацию компьютерного оборудования персонального пользования, установку необходимых для работы программных продуктов или аппаратного обеспечения, получение доступа к необходимым информационным ресурсам, к оборудованию общего пользования, а также вправе вносить предложения по изменению настоящего Регламента и Политики информационной безопасности.

**Пользователь** информационных ресурсов **обязан:**

* ознакомиться с настоящим Регламентом и Политикой информационной безопасности до начала работы на компьютерном оборудовании;
* получить личные атрибуты доступа (имя, пароль) для работы с оборудованием с установленными полномочиями;
* использовать компьютерное оборудование исключительно для деятельности, предусмотренной производственной необходимостью и должностными инструкциями;
* устанавливать компьютерное оборудование в удобном для работы месте, на прочной (устойчивой) поверхности вдали от потенциальных источников загрязнения (открытые форточки, цветочные горшки, аквариумы, чайники, вазы с цветами и прочее), так, чтобы вентиляционные отверстия средств вычислительной техники были открыты для циркуляции воздуха;
* протирать компьютерное оборудование от пыли не реже одного раза в неделю с соблюдением требований ТБ;
* незамедлительно сообщать IT-специалистам о замеченных неисправностях компьютерного оборудования и недостатках в работе программного

обеспечения общего пользования;

* рационально пользоваться ограниченными разделяемыми ресурсами (дисковой памятью компьютеров общего пользования, пропускной способностью локальной сети) и расходными материалами;
* выполнять рекомендации и указания IT-специалистов;
* незамедлительно предоставлять по запросу IT-специалистов корректную информацию об используемых сетевых программах, о пользователях, имеющих доступ к ПК или зарегистрированных в многопользовательских операционных системах;
* предоставлять беспрепятственный доступ к ПК IT-специалистам для проверки исправности и соответствия установленным правилам работы;
* незамедлительно сообщать IT-специалистам о замеченных случаях нарушения компьютерной безопасности (несанкционированный доступ к оборудованию и информации, несанкционированное искажение или уничтожение информации);
* входить в сеть при каждом сеансе работы с использованием персонального пароля и имени пользователя;
* по запросу системы выполнять команду об обновлении базы данных антивирусного ПО, следить за бесперебойной работой данного ПО, информировать IT-специалистов при обнаружении вирусов, попыток несанкционированного доступа или каких-либо подозрительных действий.

**Руководители структурных подразделений также обязаны:**

* ознакамливать подчиненных работников с настоящим Регламентом и Политикой информационной безопасности и изменениями к ним и осуществлять контроль за соблюдением их требований в возглавляемых структурных подразделениях;
* вести контроль за использованием компьютерного оборудования.

**Пользователю** информационных ресурсов **запрещается:**

* использовать оборудование для деятельности, не обусловленной производственной необходимостью и должностной инструкцией;
* создавать помехи работе других пользователей, помехи работе компьютеров и сети;
* включать, выключать, переключать, перемещать, разбирать, изменять настройку оборудования общего пользования, кроме случаев пожарной опасности (дыма из оборудования) или других угроз жизни и здоровью людей или сохранности имущества;
* подключать к локальной сети новые компьютеры и оборудование без участия IT-специалистов;
* передавать другим лицам свои личные атрибуты доступа (регистрационное имя и пароль) к компьютерному оборудованию и сети подразделения;
* осуществлять доступ к оборудованию и сети с использованием чужих личных атрибутов доступа или с использованием чужого сеанса работы;
* удалять или перемещать файлы других пользователей на серверах общего пользования;
* осуществлять попытку несанкционированного доступа к компьютерному оборудованию и информации, хранящейся на компьютерах и передаваемой по сети;
* использовать, распространять и хранить программы, предназначенные для осуществления несанкционированного доступа, взлома паролей, для нарушения функционирования компьютерного оборудования и компьютерных сетей, а также компьютерные вирусы и любые программы, ими инфицированные;
* использовать, распространять и хранить программы сетевого управления и мониторинга без специального разрешения IT-специалистов;
* использовать удаленное подключение к другим ПК;
* предоставлять доступ к компьютерному оборудованию незарегистрированным пользователям;
* использовать на своих рабочих станциях съемные накопители и прочие устройства без предварительной проверки на возможные угрозы (проникновение вирусов, вредоносных программ, вероятность физических неисправностей; в случае, когда пользователь не может самостоятельно удостовериться в отсутствии угроз, он обязан обратиться за помощью к IT-специалистам);
* удалять или изменять установленное программное обеспечение (ПО);
* устанавливать на свой компьютер ПО, не предназначенное для выполнения производственных задач;
* выполнять действия и команды, результат и последствия которых пользователю не известны;
* производить замену IP адресов и перенастройку ПК;
* устанавливать, модифицировать или хранить на ПК любое программное обеспечение без согласования с IT-специалистами;
* самостоятельно разбирать компьютерное оборудование или проводить работы по установке или обслуживанию любых других аппаратных средств;
* хранить на ПК данные не служебного характера (видео-файлы, аудио-файлы, графические файлы, игры и пр.);
* самостоятельно устанавливать (менять) пароли на доступ к информационным ресурсам учреждения, используемым совместно с другими работниками учреждения;
* запрашивать и получать из Интернета программные продукты, мультимедийные данные или изображения, кроме случаев, связанных с производственной необходимостью;
* использовать любые программные и аппаратные средства, которые могут привести к перегрузке сети или иным способом негативно повлиять на ее работу;
* использовать программы подбора паролей пользователей других компьютеров сети, сканирования адресов других пользователей, подделки служебной информации о компьютере и другое ПО, угрожающее функционированию сети или ее безопасности;
* использовать программы выявления неисправности конфигураций других компьютеров и устройств, подключенных к сети;
* вносить изменения в информационные ресурсы, не принадлежащие самому пользователю;
* подключать в электрическую сеть, предназначенную для компьютерной и офисной техники, бытовые электрические приборы (чайники, обогреватели и др.);
* использовать неисправную компьютерную и офисную технику;
* использовать неисправные розетки.

**Пользователь несет ответственность за**:

* целостность и сохранность вверенных ему информационных и аппаратных ресурсов;
* все действия, совершенные от его имени с использованием его учетной записи;
* целенаправленное блокирование работы антивирусного программного обеспечения (автоматическое обновление и автоматическую проверку по графику);
* использование служебного персонального компьютера, ЛВС и Интернет в целях, не связанных с решением производственных задач.

 **При несоблюдении пользователями требований настоящего Регламента к ним применяется меры взыскания в соответствии со степенью вины, установленной служебным разбирательством.**

 **Администраторы ЛВС** (в т.ч. IT-специалисты отдела КПРиАСУ областного ЦГЭиОЗ) обеспечивают работоспособность и информационную безопасность ЛВС, при этом они **имеют право**:

* требовать от пользователей ЛВС соблюдения установленных технологий обработки информации и выполнения инструкций по обеспечению безопасности и защите информации в ЛВС;
* делать предупреждения пользователям, нарушившим установленные правила работы, а также информировать их непосредственных руководителей о произошедшем инциденте;
* требовать от пользователя подробного отчета о работе, если во время этой работы произошел отказ или сбой оборудования или программного обеспечения общего пользования;
* проверять исправность компьютеров, подключенных к ЛВС, правильность настройки сетевых программ и соблюдение правил работы с использованием, при необходимости, доступа к ПК на время проверки;
* оперативно отключать от сети, блокировать работу или выводить из эксплуатации оборудование в случае нарушения компьютерной безопасности по причине неисправности или грубого нарушения правил работы;
* в экстренной ситуации, для обеспечения бесперебойной работы сети и компьютеров общего пользования, осуществлять отключение оборудования в отсутствие ответственного лица или пользователя и без предварительного уведомления;
* удалять без предупреждения с дисков компьютеров общего пользования файлы пользователей, содержащие игровые программы и программы, предназначенные для нарушения компьютерной безопасности, файлы, зараженные компьютерными вирусами, файлы, содержащие мультимедиа-информацию, не имеющую отношения к деятельности ЦГЭ;
* инициировать проведение служебных разбирательств по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов ЛВС;
* обращаться к пользователю или руководителю структурного подразделения с требованием прекращения работы в ЛВС при несоблюдении установленной технологии обработки информации и невыполнении требований по безопасности;
* запрашивать от руководителей подразделений и работников необходимые документы и информацию;
* вносить на рассмотрение руководителей ЦГЭ предложения по совершенствованию работы, связанной с предусмотренными настоящим Регламентом обязанностями.

**Администраторы ЛВС обязаны:**

* поддерживать работу оборудования и программного обеспечения общего пользования для обеспечения выполнения пользователями их служебных обязанностей;
* следить за стабильной работой рабочих станций, серверов, установленных на них программ и автоматизированных систем;
* следить за актуальностью учетных записей, паролей и полномочий пользователей;
* предоставлять пользователям информацию, необходимую для работы на компьютерном оборудовании общего пользования;
* доводить до сведения пользователей информацию об изменении правил или режима работы оборудования общего пользования;
* проводить среди пользователей разъяснительную работу по вопросам компьютерной безопасности;
* доводить до сведения пользователей правила работы на конкретном оборудовании;
* не разглашать информацию, полученную в ходе выполнения служебных обязанностей и не имеющую прямого отношения к выполняемым обязанностям;
* обеспечить межсетевое экранирование с использованием собственных возможностей и (или) возможностей уполномоченных поставщиков интернет-услуг;
* исключить подключение рабочего места в локальной сети к сетям связи общего пользования через другие каналы доступа (сотовый телефон, модем);
* обеспечить идентификацию абонентских устройств в локальной сети;
* обеспечить блокирование неконтролируемого обмена информацией между рабочими местами пользователей в локальной сети;
* исключить использование на рабочих местах в локальной сети постороннего программного обеспечения, ресурсов сети Интернет, предназначенных для сокрытия действий пользователя;
* обеспечить синхронизацию системного времени от единого (общего) источника (в качестве источника использовать службу единого времени Белорусского государственного института метрологии);
* сообщать заместителю главного врача по хозяйственной работе о пользовании интернетом не по назначению в форме докладной записки при обнаружении нарушения;

**Администраторы ЛВС несут ответственность за:**

* несвоевременное уведомление руководства о случаях злоупотреблений сетью;
* разглашение сведений, составляющих служебную тайну или сведений ограниченного распространения, ставших известными им по роду работы.

 **Перечень мер, принимаемых администраторами ЛВС по минимизации последствий реализации угрозы вредоносного воздействия на ИТ-инфраструктуру и медицинские информационные системы ЦГЭ:**

При эксплуатации информационных систем в ЦГЭ необходимо:

1. Использовать средства защиты информации, в том числе средства защиты от вредоносного программного обеспечения, имеющие сертификат соответствия, выданный в Национальной системе подтверждения соответствия Республики Беларусь;
2. Обеспечить регулярное автоматическое централизованное обновление антивирусных баз на всех рабочих станциях и серверах УЗ;
3. Провести полное сканирование на наличие вредоносных программ на рабочих станциях и серверах;
4. Проводить мониторинг вирусной активности на постоянной основе. Принимать неотложные меры к недопущению распространения вирусов, вплоть до отключения зараженных рабочих станций от ЛВС;
5. По возможности применять в информационной системе современные системы обнаружения и предотвращения атак, которые выявляют и блокируют в сетевом трафике как самих «шифровальщиков», так и их обращения к командным центрам;
6. Исключить наличие на рабочих станциях программного обеспечения, использование которого не предусмотрено функциональными обязанностями пользователя. Обеспечить периодическую проверку рабочих станций на предмет наличия несанкционированно установленного программного обеспечения;
7. Исключить возможность работы пользователей в информационной системе без аутентификации или под учетной записью с правами администратора системы (за исключением пользователей, которым для необходим такой доступ в соответствии с выполняемыми ими функциями). Организовать работу пользователей на рабочих станциях под персональными учетными данными (каждый пользователь работает под своей учетной записью);
8. Проводить плановую замену паролей доступа к серверам (как виртуальных, так и host-серверов). Пароль должен соответствовать следующим минимальным требованиям безопасности:

пароли не должны основываться на каком-либо одном слове, выданном идентификаторе, имени, кличке, паспортных данных, номерах страховок и т.д.;

пароли не должны основываться на типовых шаблонах и идущих подряд на клавиатуре или в алфавите символов, например, таких, как: qwerty, 1234567, abcdefgh и т.д.;

пароли должны одновременно содержать символы как минимум из трех следующих групп:

* строчные латинские буквы: abc…xyz;
* прописные латинские буквы: ABC…XYZ;
* цифры: 123…90;
* специальные символы: !%()\_+ и т.д.

Требования к длине пароля:

* для обычных пользователей ‑ не менее 5 символов;
* для администраторов (*локального/доменного*) ‑ не менее 10 символов;
* для сервисных идентификаторов ‑ не менее 10 символов;

Периодичность смены пароля:

* административные – раз в год;
* пользовательские – раз в 3 года;
* сервисные – не реже двух раз в год;

пароли не должны храниться и передаваться в незашифрованном виде по публичным сетям (*локальная вычислительная сеть, интернет, электронная почта*);

пароли нельзя записывать на бумагу, в память телефона и т.д. Нельзя сообщать, передавать кому-либо пароль.

1. Провести установку обновлений программного обеспечения, влияющего на уровень безопасности;
2. Провести разъяснительную работу с коллективом в отношении «открытия» электронных почтовых сообщений, особенно содержащих вложения и пришедших с неизвестных адресов (распространение вирусов «шифровальщиков» происходит, как правило, через почтовые отправления);
3. Обеспечить централизованное автоматическое резервное копирование информации, хранящейся на серверах, не реже 1 раза в месяц.

При создании резервной копии:

* организовать резервное копирование объектов (файлы, базы данных, образы систем, дистрибутивы, исходные коды программных средств) с целью восстановления их в случае сбоя или уничтожения;
* накопление не менее 2-х полных резервных копий по схеме: каждая четвертая копия затирает первую (последний зашел – первый вышел);
* резервные копии хранить отдельно от сервера, на котором функционирует МИС и(или) расположена база данных МИС.

**Действия руководства ЦГЭ при смене администратора ЛВС или администратора безопасности**:

При смене администратора ЛВС или администратора безопасности руководитель ЦГЭ обязан обеспечить оперативную замену всех средств аутентификации, которыми пользовался этот работник, включая:

* пароли доступа к системам;
* идентификаторы пользователей;
* ключи шифрования и сертификаты.

Это необходимо для исключения возможности несанкционированного доступа к информационным ресурсам и обеспечения непрерывности защиты данных.

**Первоочередные действия администратора ЛВС в случае инцидента информационной безопасности:**

В случае выявления инцидента (например, заражения вредоносным ПО или шифровальщиком) администратор ЛВС должен предпринять следующие первоочередные действия:

1. остановить процесс шифрования – в т.ч. при необходимости экстренно отключить питание заражённого компьютера;

2. изолировать заражённые узлы от сети (физически или логически) для предотвращения:

- распространения вируса,

- шифрования удалённых хранилищ,

- связи с командными центрами злоумышленников;

 3. провести антивирусное сканирование всех рабочих станций и серверов, при этом использовать:

- загрузку с внешнего носителя, а не из заражённой операционной системы,

- по возможности - две разные антивирусные программы для повышения вероятности обнаружения угроз.

 Категорически запрещается выполнять требования злоумышленников, включая оплату выкупа, установку сторонних программ и переход по присланным ссылкам.

**2. Требования к использованию Интернета**

Доступ в Интернет с рабочих компьютеров предоставляется только по заявке руководителя структурного подразделения и с разрешения руководителя ЦГЭ **исключительно для выполнения трудовых обязанностей, делового общения и получения информации по направлениям деятельности ЦГЭ**.

Работникам при пользовании Интернетом с рабочих мест **запрещается**:

* посещать запрещённые сайты, в том числе:
	+ экстремистские, террористические,
	+ пропагандирующие насилие, разжигающие рознь,
	+ порнографические,
	+ нарушающие законодательство;
* использовать сайты развлекательного характера, включая:
	+ социальные сети,
	+ сайты знакомств,
	+ торговые площадки,
	+ ресурсы для обмена файлами;
* скачивать или передавать авторские материалы без разрешения;
* загружать и запускать видео, аудио, программы без проверки, так как они могут содержать вредоносное ПО;
* использовать публичные мессенджеры (Viber, Telegram, WhatsApp и др.) для передачи служебной информации.

Право на размещение официальной информации о деятельности ЦГЭ посредством официальных аккаунтов ЦГЭ в соцсетях имеют только специально уполномоченные на это работники.

**3. Требования к использованию электронной почты**

Электронная почта ЦГЭ предназначена только для служебных целей, использование ее в личных или развлекательных целях запрещено.

**Не допускается**:

* использовать адреса корпоративной почты для подписок без согласования;
* указывать вымышленные обратные адреса;
* публиковать адреса ЦГЭ в открытых неофициальных интернет-ресурсах (форумы, чаты и т.д.);
* открывать вложения без антивирусной проверки, даже от известных отправителей;
* массово рассылать рекламу или «спам»;
* распространять вредоносные коды, вирусы, генераторы ключей, серийные номера, логины и пароли;
* отправлять информацию, нарушающую авторские права, содержащую патенты, торговые марки, либо иную интеллектуальную собственность без разрешения правообладателя;
* передавать сведения, нарушающие законодательство, включая:
	+ клевету, угрозы, непристойные выражения,
	+ подстрекательство к противоправным действиям,
	+ информацию с грифом «Для служебного пользования».

Работник обязан соблюдать деловой этикет при ведении электронной переписки.
При получении подозрительного письма (неизвестный отправитель, странное вложение и т.п.) работник обязан:

* не открывать вложения;
* не переходить по ссылкам;
* немедленно уведомить IT-специалиста.

**4. Правила эксплуатации офисной техники**

Работники обязаны использовать офисную технику исключительно для выполнения служебных задач.
**Необходимо соблюдать правила ее эксплуатации**, в том числе:

* не использовать бумагу с металлическими предметами (скрепками, скобами и т.п.) при печати;
* не размещать посторонние предметы в лотках и механизмах;
* соблюдать последовательность включения и выключения устройств;
* не перегружать электросети.

В случае повреждения оборудования по вине работника (в т.ч. по халатности), он может быть привлечён к материальной и дисциплинарной ответственности в соответствии с трудовым законодательством.