«Утверждаю»
Директор Дубровского детского дома-интерната
_____В.В. Паршенкова
«03» 09 2018 год

ПОЛИТИКА
информационной безопасности в ГБСУСОН «Дубровский детский дом-интернат для умственно отсталых детей»

1. Общие положения

1.1. Настоящая Политика является документом, регулирующим деятельность ГБСУСОН «Дубровский детский дом-интернат для умственно отсталых детей» (далее – Учреждение) в области информационной безопасности.
1.2. Под информационной безопасностью понимается состояние защищенности информации, характеризуемое способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность, целостность и доступность информации при ее обработке техническими средствами.
1.3. Политика информационной безопасности утверждается руководителем учреждения
1.4. Ответственность за общий контроль содержания настоящего документа и внесение в него изменений возлагается на Руководителя учреждения.

2. Цели в области информационной безопасности

В области информационной безопасности учреждения устанавливаются следующие цели:
2.1. Соответствие требованиям законодательства и договорным обязательствам в части информационной безопасности;
2.2. Повышение деловой репутации и корпоративной культуры учреждения;
2.3.Эффективное управление информационной безопасностью и непрерывное совершенствование системы управления информационной безопасностью.

3. Задачи обеспечения информационной безопасности

Для достижения основной цели защиты и обеспечения указанных свойств 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 субъектам информационных отношений, нарушению нормального функционирования информационной системы;
- создание механизма оперативного реагирования на угрозы безопасности;
- создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации;
- защиту от вмешательства в процесс функционирования информационной системы посторонних лиц (доступ к информационным ресурсам должны иметь только допущенные к ОПД сотрудники);
- разграничение доступа пользователей к информационным, аппаратным, программным и

иным ресурсам (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы для выполнения служебных обязанностей), то есть защиту от несанкционированного доступа;
- защиту от несанкционированной модификации используемых в информационной системе программных средств, а также защиту системы от внедрения несанкционированных программ, включая компьютерные вирусы;
- защиту информации ограниченного пользования от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи;
- обеспечение живучести криптографических средств защиты информации.

Основные пути решения задач системы защиты:

Поставленные основные цели защиты и решение перечисленных выше задач достигаются:
- учетом всех подлежащих защите ресурсов информационной системы (информации, задач, документов, каналов связи, серверов, автоматизированных рабочих мест);
- полнотой, реальной выполнимостью и непротиворечивостью требований документов по вопросам обеспечения безопасности информации;
- подготовкой должностных лиц (сотрудников), ответственных за организацию и осуществление практических мероприятий по обеспечению безопасности информации и процессов ее обработки;
- наделением каждого сотрудника (пользователя) минимально необходимыми для выполнения им своих функциональных обязанностей полномочиями по доступу к информационным ресурсам;
- четким знанием и строгим соблюдением всеми пользователями информационной системы требований документов по вопросам обеспечения безопасности информации;
- персональной ответственностью за свои действия каждого сотрудника, в рамках своих функциональных обязанностей имеющего доступ к информационным ресурсам;
- непрерывным поддержанием необходимого уровня защищенности элементов информации;
- применением физических и технических (программно-аппаратных) средств защиты ресурсов системы;
- эффективным контролем за соблюдением пользователями информационных ресурсов, требований по обеспечению безопасности информации.

4. Основные принципы построения системы информационной безопасности

Построение системы, обеспечения безопасности информации, и ее функционирование должны осуществляться в соответствии со следующими основными принципами:
- законность;
- системность;
- комплексность;
- непрерывность;
- своевременность;
- персональная ответственность;
- исключение конфликта интересов;
- взаимодействие и сотрудничество;
- простота применения средств защиты;
- обязательность контроля.

Законность

Предполагает осуществление защитных мероприятий и разработку системы безопасности информации в соответствии с действующим законодательством в области информации, информатизации.

Системность

Системный подход к построению системы защиты информации предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности информации.

Комплексность

Комплексное использование методов и средств защиты компьютерных систем предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов.

Непрерывность защиты

Обеспечение безопасности информации - процесс, осуществляемый руководителем и сотрудниками допущенными к ОПД. Это не только и не столько процедура или политика, которая осуществляется в определенный отрезок времени или совокупность средств защиты, сколько процесс, который должен постоянно идти на всех уровнях. Деятельность по обеспечению информационной безопасности является составной частью повседневной деятельности учреждения.

Своевременность

Предполагает упреждающий характер мер обеспечения безопасности информации, то есть постановку задач по комплексной защите информации и реализацию мер обеспечения безопасности информации.

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.

Исключение конфликта интересов (разделение функций)

Эффективная система обеспечения информационной безопасности предполагает четкое разделение обязанностей сотрудников и исключение ситуаций, когда сфера ответственности сотрудников допускает конфликт интересов.

Взаимодействие и сотрудничество

Предполагает создание благоприятной атмосферы в коллективах структурных подразделений. В такой обстановке сотрудники должны осознанно соблюдать установленные правила и оказывать содействие деятельности подразделений защиты информации.

Важным элементом эффективной системы обеспечения безопасности информации является высокая культура работы с информацией, соблюдение этических норм и стандартов профессиональной деятельности, создание корпоративной культуры, подчеркивающей и демонстрирующей персоналу на всех уровнях важность обеспечения информационной безопасности.

Простота применения средств защиты

Механизмы и методы защиты должны быть интуитивно понятны и просты в использовании. Применение средств и методов защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций.

Обязательность 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.
Недостатки системы обеспечения информационной безопасности, выявленные сотрудниками должны немедленно доводиться до сведения руководителя.

5. Ответственность за реализацию политик информационной безопасности

Ответственность за разработку мер и контроль обеспечения защиты информации несёт ответственный за ОПД и руководитель Учреждения.
Ответственность за реализацию политик возлагается:
- в части, касающейся разработки и актуализации правил внешнего доступа, антивирусной защиты, а также доведения правил политик до сотрудников;
- в части, касающейся исполнения правил политики, – на каждого сотрудника, согласно их должностным и функциональным обязанностям, и иных лиц, попадающих под область действия настоящей политики.

6. Порядок подготовки персонала по вопросам информационной безопасности и допуска его к работе

Организация просвещения сотрудников в области информационной безопасности возлагается на ответственного за ОПД. Подписи сотрудников об ознакомлении заносятся в лист ознакомления. Обучение сотрудников правилам обращения с конфиденциальной информацией, проводится путем:
- проведения инструктивных занятий;
- самостоятельного изучения сотрудниками внутренних нормативных документов.
Допуск персонала к работе с защищаемыми информационными ресурсами осуществляется только после его ознакомления с настоящими политиками, а так же иными инструкциями пользователя информационных систем. Согласие на соблюдение правил и требований настоящей политики подтверждается подписями сотрудников.

7. Профилактика нарушений политик информационной безопасности

Под профилактикой нарушений политик информационной безопасности понимается проведение регламентных работ по защите информации, предупреждение возможных нарушений информационной безопасности и проведение разъяснительной работы по информационной безопасности среди пользователей.
Проведение в ИС регламентных работ по защите информации предполагает выполнение процедур контрольного тестирования (проверки) функций СЗИ, что гарантирует ее работоспособность с точностью до периода тестирования.
Задача предупреждения в ИС возможных нарушений информационной безопасности решается по мере наступления следующих событий:
- включение в состав ИС новых программных и технических средств, при условии появления уязвимых мест в ИС учреждения;
- изменение конфигурации программных и технических средств ИС;
- при появлении сведений о выявленных уязвимых местах в составе операционных систем и/или программного обеспечения технических средств, используемых в ИС.
Ответственный за ОПД собирает и анализирует информацию о выявленных уязвимых местах в составе операционных систем и/или программного обеспечения относительно ИС.
Ответственный за ОПД организовывает периодическую проверку ИС путем моделирования возможных попыток осуществления НСД к защищаемым информационным ресурсам.

Для решения задач контроля защищенности ИС используются инструментальные средства для тестирования реализованных в составе ИС средств и функций защиты.
Плановая разъяснительная работа по правилам настоящих политик, а также инструктаж сотрудников по соблюдению требований нормативных и регламентных документов по информационной безопасности, проводится ответственным за ОПД.
Прием на работу новых сотрудников должен сопровождаться ознакомлением их с правилами и требованиями настоящей политики.

8. Ликвидация последствий нарушения политик информационной безопасности

Ответственный за ОПД, используя данные, полученные в результате применения инструментальных средств контроля (мониторинга) безопасности информации ИС, должен своевременно обнаруживать нарушения информационной безопасности, факты осуществления НСД к защищаемым информационным ресурсам и предпринимать меры по их локализации и устранению.
В случае обнаружения подсистемой защиты информации факта нарушения информационной безопасности или осуществления НСД к защищаемым информационным ресурсам ИС рекомендуется уведомить ответственного за ОПД и/или руководителя, и далее следовать их указаниям.
Действия ответственного за ОПД при признаках нарушения политик информационной безопасности регламентируются следующими внутренними документами:
- Инструкцией пользователя ИСПД;
- Политикой информационной безопасности;
- Должностными обязанностями.

После устранения инцидента необходимо составить акт о факте нарушения и принятых мерах по восстановлению работоспособности ИС, а также зарегистрировать факт нарушения в журнале учета нарушений, ликвидации их причин и последствий.

9. Ответственность за нарушение Политики информационной безопасности

Ответственность за выполнение правил Политик безопасности несет каждый сотрудник допущенный к ОПД в рамках своих служебных обязанностей и полномочий.
На основании ст. 192 Трудового кодекса РФ сотрудники, нарушающие требования политики безопасности, могут быть подвергнуты дисциплинарным взысканиям, включая замечание, выговор и увольнение с работы.
Все сотрудники допущенные к ОПД несут персональную (в том числе материальную) ответственность за прямой действительный ущерб, причиненный учреждению в результате нарушения ими правил политики ИБ (Ст. 238 Трудового кодекса РФ).
За неправомерный доступ к компьютерной информации, создание, использование или распространение вредоносных программ, а также нарушение правил эксплуатации ЭВМ, следствием которых явилось нарушение работы ЭВМ (автоматизированной системы обработки информации), уничтожение, блокирование или модификация защищаемой информации, сотрудники несут ответственность в соответствии со статьями 272, 273 и 274 Уголовного кодекса Российской Федерации.