Муниципальное бюджетное дошкольное образовательное учреждение детский сад общеразвивающего вида № 11 «Рябинка» Новоалтайска Алтайского края

Приложение №__ к приказу
от _____20____г
Заведующий
МБДОУ детского сада № 11
_____Т.В. Лисица

11» января 2016 г.

ПОЛОЖЕНИЕ

об обеспечении безопасности автоматизированной информационной системы МБДОУ детского сада № 11

1. Общие положения

1.1. Настоящее Положение определяет систему взглядов на проблему обеспечения безопасности информации в единой информационной телекоммуникационной системе (далее автоматизированной системе - АС) МБДОУ детского сада № 11 (далее ДОУ) и представляет собой систематизированное изложение целей и задач защиты, а также принципов и способов достижения требуемого уровня безопасности информации.

1.2. Построение системы безопасности АС основывается на комплексном подходе, доказавшем свою эффективность и надежность. Комплексный подход ориентирован на создание защищенной среды обработки информации в АС, сводящей воедино разнородные меры противодействия угрозам. Сюда относятся правовые, морально-этические, организационные, программные и технические способы обеспечения информационной безопасности.

1.3. Принцип построения системы безопасности АС должен быть основан на научных предпосылках.

1.4. Правовой базой для разработки Положения служат требования действующих в России законодательных и нормативных документов: Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»; Постановление Правительства Российской Федерации от 17.11.2007. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», а также нормативно-методические материалы и организационно-распорядительные документы ДОУ, отражающие вопросы обеспечения информационной безопасности автоматизированной системы.

1.5. Положение является методологической основой для формирования и проведения в ДОУ единой политики в области обеспечения безопасности информации (политики безопасности), для принятия управленческих решений и разработки практических мер по ее воплощению.

2. Объекты защиты

2.1. Основными объектами информационной безопасности в ДОУ являются:

- информационные ресурсы с ограниченным доступом, составляющие семейную тайну, иные чувствительные по отношению к случайным и несанкционированным воздействиям и нарушению их безопасности информационные ресурсы, в том числе открытая (общедоступная) информация,

представленные в виде документов и массивов информации, независимо от формы и вида их представления;

- процессы обработки информации в АС - информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации;

- информационная инфраструктура, включающая системы 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 чувствительные компоненты АС

2.2. Цели создания и эксплуатация АС как объекта информатизации: повышение качества процесса обработки персональных данных, контроля, оперативности, анализа и прогноза;

2.3. Структура, состав и размещение основных элементов АИС, информационные связи с другими объектами:

2.3.1. какие взаимосвязи прослеживаются между различными объектами АИС, какие технические средства используются, есть ли взаимодействие с внешними организациями и как это происходит, т.е. какие каналы передачи данных используем, какое ПО для этого необходимо

2.4. Категории информационных ресурсов, подлежащих защите:

- персональные данные сотрудников ДОУ;

- персональные данные обучающихся, воспитанников и их родителей (законных представителей);

- персональные данные сотрудников, являющихся материально ответственными лицами;

- персональные данные опекунов, опекаемых и подопечных;

- персональные данные доверенных лиц родителей (законных представителей) воспитанников\

2.5. Категории пользователей АС, режимы использования и уровни доступа к информации:

2.5.1. лицо, отвечающее за организацию мер по защите персональных данных, выступает в роли администратора;

2.5.2. лица, имеющие доступ к обработке персональных данных, могут выступать только в роли руководителя. Доступ к автоматизированной информационной системе в роли пользователя и редактора не позволяет специалисту выполнять функции, прописанные в его должностных обязанностях.

3. Цели и задачи защиты персональных данных

3.1. Основная цель, на достижение которой направлены все разделы настоящего Положения: защита субъектов информационных отношений (интересы которых затрагиваются при создании и функционировании АИС) от возможного нанесения им ощутимого материального, физического, морального или иного ущерба посредством случайного или преднамеренного несанкционированного вмешательства в процесс функционирования АИС или несанкционированного доступа к циркулирующей в ней информации и ее незаконного использования.

3.2. Основные задачи системы обеспечения безопасности информации:

- защита от вмешательства в процесс функционирования АС;
- разграничение прав доступа к информации, персональным компьютерам, средствам защиты;
- регистрация происходящих событий в АИС, процедуры обеспечения целостности и достоверности информации;
- методы восстановления информации;
- защита от несанкционированных действий;
- авторизация и аутентификация пользователей;
- мониторинг возможных угроз и информационной защищенности; действия для минимизации и локализации ущерба от неправомерных действий.

3.3. Основные пути достижения целей защиты:

- строгий учет всех подлежащих защите ресурсов системы (информации, задач, каналов связи, серверов, автоматизированных рабочих мест - АРМ);

- создание полных, реально выполняемых и непротиворечивых требований организационно-распорядительных документов ДОУ по вопросам обеспечения безопасности информации;

- осознание персональной ответственности за свои действия каждого сотрудника, участвующего в рамках своих функциональных обязанностей, в процессах автоматизированной обработки информации и имеющего доступ к ресурсам АС;

- реализация технологических процессов обработки информации с использованием комплексов организационно-технических мер защиты программного обеспечения, технических средств и данных;

- принятие эффективных мер обеспечения физической целостности технических средств и непрерывным поддержанием необходимого уровня защищенности компонентов АС;

- применение физических и технических (программно-аппаратных) средств защиты ресурсов системы и непрерывной административной поддержкой их использования;

- осуществление юридической защиты интересов ДОУ при взаимодействии ее подразделений с внешними организациями (связанном с обменом информацией) от противоправных действий, как со стороны этих организаций, так и от несанкционированных действий обслуживающего персонала и третьих лиц;

- проведение постоянного анализа эффективности и достаточности принятых мер и применяемых средств защиты информации, разработка и реализация предложений по совершенствованию системы защиты информации в АС.

4. Основные угроза безопасности информации

Виды угроз информационной безопасности и их источники.

4.1. Наиболее значимые угрозы:

- нарушение конфиденциальности (разглашение, утечка);
- нарушение работоспособности (дезорганизация работы);

- нарушение целостности (искажение, подмена, уничтожение).

4.2. Основные источники угроз:

- непреднамеренные (ошибочные, случайные, необдуманные, без злого умысла и корыстных целей);
- преднамеренные (в корыстных целях, по принуждению третьими лицами, со злым умыслом и т.п.);
- воздействия из других логических и физических сегментов АС со стороны сотрудников других подразделений;
- ошибки, допущенные при проектировании АС;
- аварии, стихийные бедствия и т.п.

5. Пути осуществления направлений технической политики

5.1. реализация разрешительной системы допуска пользователей к информации;

5.2. разграничение доступа пользователей к информационным ресурсам;

5.3. реализация системы сбора, обработки, объективное документирование событий;

5.4. регистрация действий пользователей и контроль за несанкционированным доступом и действиями пользователей;

5.5. надежное хранение традиционных и машинных носителей информации.

6. Комплексы мер по формированию режима безопасности информации

6.1. Организационно-правовой режим:

создание и поддержание правовой базы безопасности информации и разработку (введение в действие) необходимых организационно-распорядительных документов (перечень сведений конфиденциального характера, приказы по установлению режима безопасности информации, инструкции и функциональные обязанности сотрудников и другие нормативные документы).

6.2. Технические и программные мероприятия: физическая охрана объектов информации, защита информации ограниченного распространения от утечки по техническим каналам, выполнение режимных требований при работе с информацией ограниченного распространения и мероприятия технического контроля.

7. Принципы построения комплексной системы защиты

7.1. законность: предполагает осуществление защитных мероприятий и разработку системы безопасности информации АС комитета по образованию в соответствии с действующим законодательством;

7.2. системность: системный подход к построению системы защиты информации предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности информации;

7.3. 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, защита должна строиться эшелонированно;

7.4. непрерывность защиты: непрерывный, целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла АС;

7.5. своевременность: предполагает упреждающий характер мер для обеспечения безопасности информации;

7.6. преемственность и совершенствование: предполагают постоянное совершенствование мер и средств защиты информации;

7.7. разумная достаточность (экономическая целесообразность); предполагает соответствие уровня затрат на обеспечение безопасности информации ценности информационных ресурсов и величине возможного ущерба;

7.8. персональная ответственность: предполагает возложение ответственности за обеспечение безопасности информации и системы ее обработки на каждого сотрудника в пределах его полномочий;

7.9. принцип минимизации полномочий: означает предоставление пользователям минимальных прав доступа в соответствии с производственной необходимостью;

7.10. взаимодействие и сотрудничество; предполагает создание благоприятной атмосферы в коллективе;

7.11. гибкость системы защиты: для обеспечения возможности варьирования уровня защищенности средства защиты должны обладать определенной гибкостью;

7.12. открытость алгоритмов и механизмов защиты: суть данного принципа состоит в том, что защита не должна обеспечиваться только за счет секретности. Знание алгоритмов работы системы защиты не должно давать возможности ее преодоления (даже авторам), однако это не означает, что информация о конкретной системе защиты должна быть общедоступна;

7.13. простота применения средств защиты: механизм защиты должны быть интуитивно понятен и прост в использовании, без значительных дополнительных трудозатрат;

7.14. научная 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, научно обоснованы с точки зрения достижения заданного уровня безопасности информации и должны соответствовать установленным нормам и требованиям по безопасности информации;

7.15. обязательность контроля: предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил безопасности.

8. Меры, методы и средства защиты

8.1. правовые (законодательные): разработка локальных актов

8.1.1. Положение о защите персональных данных, обрабатываемых ДОУ.

8.1.2. Положение об ответственном лице за информационную безопасность.

8.1.3. Положение об организации парольной защиты при обработке персональных данных и иной конфиденциальной информации.

8.1.4. Приказ о допуске сотрудников ДОУ к обработке персональных данных.

8.1.5. Приказ ДОУ о назначении лиц, ответственных за организацию мер по защите персональных данных.

8.1.6. Приказ об утверждении мест хранения персональных данных, обрабатываемых ДОУ.

8.1.7. Регламент присвоения прав доступа к автоматизированной информационной системе.

8.1.8. Регламент работы сотрудников ДОУ с электронной почтой.

8.1.9. Регламент использования ресурсов глобальной сети Интернет в ДОУ.

8.1.10. инструкция по правилам обработки персональных данных работника ДОУ.

8.1.11. Инструкция по правилам обработки персональных данных субъектов, осуществляемой сотрудниками ДОУ.

8.1.12. Инструкция по организации антивирусной защиты автоматизированной информационной системы ДОУ.

8.2. морально-этические,

8.3. организационные (административные): разработка плана мероприятий по обеспечению мер защиты информации от несанкционированного доступа

8.4. физические, технические (аппаратурные и программные).