Муниципальное бюджетное дошкольное образовательное учреждение «Детский сад № 2 «Рябинка» 964760 Россия Сахалинская область с.Горнозаводск, ул. Кольцевая, 31, тел (424 36) 96-517 факс (424 36) 96-517. Регистрационный № 74-009-001115; ИНН 6505009920; КПП 650501001

Утверждено приказом руководителя
МБДОУ «Детский сад №2 «Рябинка»
_____ Петрова Ю.В.
от 11.01.2017г.№ 7

ПОЛИТИКА ИНФОРМАЦИОНОЙ БЕЗОПАСНОСТИ
в МБДОУ «Детский сад №2 «Рябинка»
1. Общие положения

1.1. Политика информационной безопасности (далее – Политика) Муниципального Бюджетного Дошкольного Образовательного Учреждения «Детский сад №2 «Рябинка» (далее – Учреждение) описывает:

1.1.1. организационные меры в Учреждении по:

- формированию в Учреждении должного отношения к информации и обращению с ней;
- определению ценности информации;
- обеспечению информационной безопасности;
- определению ответственности должностных лиц по защите информации и распределению связанных с этим организационных обязанностей;

1.1.2. правила поведения сотрудников Учреждения в рамках пользования информационными ресурсами, а также основные положения защиты информации.

1.2. Настоящая Политика имеет следующие цели:

- доведение до сведения сотрудников Учреждения важности обеспечения информационной безопасности;
- формулирование целей, задач и объектов защиты, а также необходимых уровней безопасности;
- определение обязанностей подразделений и должностных лиц Учреждения по обеспечению безопасности информации.

1.3. Положения настоящей Политики являются основополагающими для разработки внутренних руководящих документов, касающихся взаимодействия с информационными ресурсами в Учреждение и должны быть доведены до всех сотрудников под подпись.

2. Значение информационной безопасности

Обеспечение информационной безопасности одной из важнейших задач для всех сотрудников Учреждения. Состояние информационной безопасности в значительной мере определяется исполнительской дисциплиной, культурой обращения с документами содержании информацию ограниченного доступа.

2.1. Согласно действующему законодательству в Учреждении выделяются следующие категории информации:

- общедоступная информация, которая в соответствии с Федеральным законом Российской Федерации № 149-ФЗ от 27.07.2006 «Об информации, информационных технологиях и о защите информации», является открытым государственным информационным ресурсом Учреждения;
- информация, доступ к которой ограничен федеральными законами – информация ограниченного доступа (информация, отнесенная к государственной тайне, конфиденциальная информация, персональным данным).

2.2. Информационные ресурсы Учреждения, в том числе информацию ограниченного доступа, запрещается передавать каким-либо способом любому физическому или юридическому лицу без согласования с руководством.

2.3. Учреждение обязано соблюдать политику лицензионного программного обеспечения и законодательства РФ. Любое неправомерное хранение, распространение и использование программного обеспечения (независимо от того, является ли оно коммерческим или свободно распространяемым) является нарушением настоящей Политики.

3. Уровень защиты информации

3.1. Правила использования, передачи и хранения информации различных категорий базируются на следующих общих принципах:

- общедоступная информация – должна защищаться и идентифицироваться стандартными средствами защиты (разграничение доступа) среды её использования, хранения или передачи таким образом, чтобы обеспечить к ней только авторизованный доступ. Для обеспечения целостности и доступности указанной информации включение информационных систем Учреждения, в которых она формируется, в состав объектов международного информационного обмена осуществляется только при использовании сертифицированных средств защиты информации;
- информация ограниченного доступа – должна защищаться и идентифицироваться дополнительными средствами (шифрование и использование электронной подписи, защита от утечки по техническим каналам), чтобы обеспечить гарантированную доставку при обработке информации только авторизованным лицам. Обработка и хранение информации ограниченного допуска производится на средствах вычислительной техники, не имеющих выход в сети международного информационного обмена и аттестованных в установленном порядке.

Информация ограниченного доступа не может быть размещена на любых, публично доступных в Интернет носителях (FTP, WWW и т.д.). Передача такой информации в другие органы власти (организации) производится в порядке, установленном законами Российской Федерации, нормативными документами Сахалинской области и Учреждения.

3.2. Достаточный уровень защиты информации определяется исходя из оценки риска реализации угроз информационной безопасности. При необходимости, для достижения такого уровня защищенности информации в Учреждении должны

применяться соответствующие методы выявления угроз, расчета рисков информационной безопасности и специальные средства для снижения или исключения этих рисков.

Технические решения по защите, принимаемые при проектировании и создании информационных систем, должны быть достаточными и подтверждаться при проведении (при необходимости) их аттестации на соответствие действующим на территории Российской Федерации нормативным документам, установленным требованиям руководящих документов и норм эффективности защиты информации.

3.3. Руководитель Учреждения обеспечивает реализацию мер по защите информации в соответствии с действующими на территории Российской Федерации законами, нормативными документами, установленными требованиями руководящих документов и норм эффективности защиты информации, а также в соответствии с разработанными на их основе внутренними требованиями.

4. Цели и задачи обеспечения информационной безопасности

4.1. Обеспечение информационной безопасности Учреждения предполагает подчиненное единому замыслу эффективное информационное обслуживание и управление всеми средствами комплексной защиты информации, адекватное отражение угроз информационной безопасности.

Главная цель принимаемых мер защиты информации состоит в том, чтобы гарантировать целостность, достоверность, доступность и конфиденциальность информации во всех ее видах и формах, включая документы и данные, обрабатываемые, хранимые и передаваемые в информационных вычислительных и телекоммуникационных системах (далее - Информационные системы), независимо от типа носителя этих данных. Организация информационных ресурсов должна обеспечивать их достаточную полноту, точность и актуальность, чтобы удовлетворять потребности Учреждения, не нарушая при этом основные принципы информационной безопасности, описанные в настоящей Политике.

4.2. В целях обеспечения информационной безопасности Учреждения необходимо выполнение следующих условий:

4.2.1. Все участники (пользователи) информационного обмена, индивидуально, должны быть зарегистрированы в рамках локальной вычислительной сети Учреждения, то есть иметь имя и пароль, позволяющие их однозначно идентифицировать, при этом:

- имя (USER NAME) участника формируется администратором локальной вычислительной сети исходя из правил, установленных в Учреждении;

- пароль пользователя выбирается участником информационного обмена самостоятельно, должен состоять не менее чем из 8 символов и включать в себя как буквы, символы так и цифры (например – K$28b%6A). Пароль является конфиденциальной информацией и не должен раскрываться никому. Пароль рекомендовано менять не реже 1 раз в 3 месяца, а в случае его компрометации – немедленно. Установка и смена пароля осуществляются пользователем самостоятельно. Обучение по вопросам установки и смены пароля организуется администратором локальной вычислительной сети;

- в случае несанкционированного доступа к защищаемой информации, осуществленного с использованием имени и пароля, всю ответственность несет владелец данного имени и пароля;

- все пароли доступа к серверам, цифровым телефонным станциям и другим, важным с точки зрения безопасности, информационным системам Учреждения должны меняться ответственным администратором локальной вычислительной сети не реже чем 1 раз в 3 месяца и храниться в подразделении (у специалиста) по информационной безопасности в запечатанных конвертах на случай необходимости оперативного подключения к информационным системам.

4.2.2. Все используемые в Учреждении информационные ресурсы должны быть классифицированы. Все документы должны быть систематизированы и учтены и для них определен строгий порядок использования, хранения, архивации и уничтожения, при котором любой документ можно быстро найти и проконтролировать его исполнение.

4.2.3. В базе информационных ресурсов Учреждения создаются перечни документов и данных (или их группы) ограниченного доступа и им присваиваются соответствующие грифы (пометка, класс) конфиденциальности. Перечни сведений, отнесенных к государственной тайне, утверждены Президентом Российской Федерации, а перечни сведений конфиденциального характера и перечень персональных данных – нормативными актами Учреждения.

4.2.4. В Информационных системах Учреждения должна обеспечивается требуемая безопасность, соответствующая критичности обрабатываемой, хранимой и передаваемой информации. Все системы должны иметь документальную оценку уровня безопасности, в системах с низким уровнем безопасности не должна обрабатывается информация более высокого уровня конфиденциальности, чем это допустимо.

4.2.5. Для всех критичных информационных систем, администратором локальной вычислительной сети, должны быть разработаны планы обеспечения непрерывной работы и восстановления при аварийных ситуациях. Эти планы должны поддерживаться в актуальном состоянии, а назначенные исполнители должны быть обучены необходимым действиям.

4.2.6. Все сотрудники Учреждения ознакомлены с требованиями Инструкции по делопроизводству (при необходимости с Инструкциями по работе со сведениями ограниченного доступа), а также обучены правилам работы в Информационных системах, обеспечены необходимым руководствами и должностным инструкциями, отражающими обязанности и процедуры по поддержанию информационной безопасности, в том числе и при взаимодействии с различными внешними организациями, информационно-аналитическими службами, средствами массовой информации.

5. Ответственность и обязанности

Сотрудники следующих уровней несут ответственность за реализацию настоящей Политики и достижение сформулированных в ней целей в Учреждении.

5.1. Управленческий уровень:

5.1.1. Руководители структурных подразделений Учреждения отвечают за:

- выполнение в пределах своей компетенции требований документов, регламентирующих обеспечение информационной безопасности, положений и правил безопасности, разработанных на основе настоящей Политики;
- информационное обеспечение, создание условий, обеспечивающих безопасную обработку информации в подразделении, в том числе сведений ограниченного доступа;
- обеспечение режима информационной безопасности и взаимодействие в этой области с подразделением (специалистом) по информационной безопасности.

5.1.2. Они обязаны:

- выполнять требования действующих нормативных документов в области информационной безопасности и требовать этого от своих подчиненных;
- знать, что деятельность их подчиненных по реализации или модернизации информационных систем без разработки, согласования и утверждения в установленном порядке проектной и эксплуатационной технической документации является нарушением основных принципов информационной безопасности;
- организовывать обучение сотрудников основам информационной безопасности таким образом, чтобы можно было гарантировать знание ими настоящей Политики и необходимых нормативных документов;

- своевременно информировать администратора локальной вычислительной сети об изменениях статуса каждого из своих подчиненных - пользователей систем, связанных с изменением функциональных обязанностей, режима работы и требуемых полномочий доступа;

- своевременно информировать руководителя Учреждения о нарушениях подчиненными установленных правил информационной безопасности, добиваться неукоснительного их соблюдения;

- обеспечить закрепление каждого компьютера в подразделении за ответственным пользователем, отвечающим за его безопасность.

5.2. Административный уровень:

5.2.1. Администраторы локальных вычислительных сетей, информационных систем обеспечивают их эффективное функционирование и отвечают за реализацию технических и организационных мер по обеспечению требований безопасности по конкретным информационным системам, за корректное применение штатных механизмов защиты системных и информационных ресурсов и использование своих администраторских привилегий.

5.2.2. Они обязаны:

- организовывать и обеспечивать создание и эксплуатацию информационных систем в соответствии с требованиями информационной безопасности, обеспечивать реализацию организационных и программно-технических мер защиты информации, участвовать в разработке локальных политик безопасности Информационных систем, сервисов и приложений;

- осуществлять своевременное и подробное документирование информационных систем, структурирование информационных ресурсов по уровням критичности, регламентировать технологию обработки, хранения и передачи информации;

- проводить оценку стоимости возможного ущерба от уничтожения или искажения профильной для своего подразделения информации или нарушения ее конфиденциальности, принимать меры по выявлению уязвимых мест систем и их устранению;

- управлять полномочиями доступа всех пользователей к функциям, сетевым, системным и информационным ресурсам в соответствии с действующими требованиями безопасности. Назначать уникальные идентификаторы и начальные пароли (или другую идентификационную и аутентификационную информацию) каждому пользователю только после того, как будет оформлена надлежащая документация.

- разрабатывать мероприятия по обеспечению целостности и неизменности программного обеспечения и данных, регулярному резервному копированию информационных ресурсов, обеспечению непрерывной работы информационных систем и восстановления их при авариях и стихийных бедствиях;

- контролировать состояние защищенности сетей, систем и приложений, оперативно и эффективно реагировать на события, влияющие на безопасность информации, своевременно выявлять и пресекать попытки нарушения защиты. Информировать руководителей структурных подразделений, подразделения (специалиста) по информационной безопасности и представлять материалы для расследования инцидентов;

- использовать средства мониторинга и аудита для обнаружения подозрительных ситуаций, периодически анализировать регистрационную системную информацию, относящуюся к безопасности сети, систем и приложений, вести архив регистрационной системной информации;

- планировать и периодически проводить проверку надежности защиты, достоверности системного программного обеспечения и целостности критичной информации.

- не допускать появления и распространения в информационных системах органов исполнительной власти и аппарата Губернатора и Правительства Сахалинской области программного обеспечения, не входящее в перечень типового, использующее ресурсы сети Правительства Сахалинской области (серверное оборудовании, сетевые хранилища, каналы связи и т.п.) без согласования с агентством по информационным технологиям и связи Сахалинской области.

5.3. Пользовательский уровень:

5.3.1. Пользователи лично отвечают за свои действия при обращении с информацией и при работе в информационных системах.

5.3.2. Они обязаны:

- знать и соблюдать установленные в Учреждении правила и порядок обработки информации. Выполнять указания должностных лиц, отвечающих за информационную безопасность, ставить в известность администратора и руководство обо всех инцидентах информационной безопасности;

- использовать информационные системы в соответствии с настоящей Политикой, требованиями безопасности к конкретным системам и приложениям. Использовать доступные защитные механизмы для обеспечения целостности и конфиденциальности информации;

- правильно относить создаваемые документы или разделы данных к соответствующему уровню конфиденциальности, а также правильно выбирать из числа доступных защищенные системы для обработки или передачи информации ограниченного доступа;

- знать признаки нестандартного поведения конкретных информационных систем и последовательность дальнейших действий;

- использовать в работе на персональных компьютерах только учтенные носители информации Учреждения. Не выносить их за пределы административного здания без согласования с руководителем подразделения;

- не использовать и не распространять в информационных системах Учреждения сторонне программное обеспечение;

- обеспечивать корректное поведение в локальной вычислительной сети, не предпринимать каких-либо действий по обходу или блокированию механизмов безопасности, по намеренному изменению, уничтожению, чтению или передаче информации неавторизованным способом. Не препятствовать получению другими пользователями авторизованного доступа к ресурсам информационной системы и информации в ней;

- информировать руководство и подразделение (специалиста) по информационной безопасности о неправомерных действиях других пользователей, нарушающих установленные правила информационной безопасности.

6. Оповещение о проблемах информационной безопасности

Необходимо немедленно сообщить в подразделение (специалисту) по информационной безопасности, администратору сети, а также руководителю структурного подразделения, если:

- информация в Учреждении утеряна, осуществлен несанкционированный доступ к информации ограниченного доступа или есть подозрение такового;

- имеют место признаки нестандартной работы персонального компьютера или программного обеспечения;

- имеют место признаки вредоносного программного обеспечения;

- был раскрыт пароль или любой другой механизм контроля доступа или есть соответствующие подозрения.

Подробности проблем и защиты информации не должны придаваться широкой огласке.

Сотрудникам Учреждения, за исключением администраторов информационных систем (сетей), запрещается проводить проверки защищенности элементов локальных вычислительных сетей и других электронных систем, а также разглашать информацию о принципах политики информационной безопасности.

7. Санкции

Несоблюдение требований документов, регламентирующих обеспечение информационной безопасности, может подвергнуть информацию недопустимому риску потери конфиденциальности, целостности или доступности при ее хранении, обработке или передаче в Информационной системе (системе документооборота) и тем самым нанести ущерб Учреждению.

Нарушения стандартов, правил, руководств или процедур, поддерживающих настоящую Политику, находятся в зоне внимания Учреждения и могут привести к дисциплинарной (административной, уголовной) ответственности нарушителей.

8. Реализация политики

8.1. Для обеспечения информационной безопасности в Учреждении разрабатывается и реализуется система защиты информации (далее – СЗИ). Создание СЗИ является одной из основных задач, в решении которой принимают участие все структурные подразделения.

Объектом СЗИ является циркулирующая, обрабатываемая, хранимая и передаваемая в Учреждении информация, и поддерживающая ее инфраструктура. СЗИ реализуется комплексом правовых, режимных, организационных и программно-технических мер.

8.2. Правовые меры защиты:

в себя следующие правовые меры:

- внесение в Положение об Учреждении положений о защите информации;
- оформление письменного обязательства о неразглашении информации ограниченного доступа;
- определение на основании законодательства Российской Федерации санкций за нарушение требований по защите информации;
- наличие в Положениях о структурных подразделениях и должностных регламентах обязанностей по защите информации;
- разработку и введение в действие требований и инструкций по обеспечению информационной безопасности.

8.3. Режимные меры защиты:

К таким мерам относятся мероприятия по регламентации, установлению, поддержанию и осуществлению контроля за состоянием:

- физической охраны (контрольно-пропускной режим перемещения ценностей, грузов, персонала, посетителей, защиты руководителей и сотрудников);
- охраны сведений различного уровня конфиденциальности;
- защиты технологических процессов, информационных ресурсов, информации и поддерживающей их инфраструктуры.

8.4. Организационные меры защиты:

К организационным мерам защиты относятся административные и процедурные мероприятия по:

- регламентации обработки, хранения и передачи информации как внутри Учреждения, так и при взаимодействии с внешними организациями, обращения с документами и носителями, порядка их учета, хранения и уничтожения;

- организации непрерывного процесса контроля (мониторинга) событий безопасности для своевременного выявления и пресечения попыток несанкционированного доступа к защищаемой информации;

- установлению правил доступа на объекты, в помещения, в Информационные системы, применению в этих целях систем охраны и управления доступом;

- формированию участков администрирования безопасности, мониторинга и аудита, политики и процедур управления доступом к защищаемым ресурсам;

- организации проектирования, строительства и оснащения объектов и информационных систем в соответствии с требованиями информационной безопасности;

- формированию условий и технологических процессов обработки, хранения и передачи информации различного уровня конфиденциальности (включая условия хранения распечаток и архивов), отвечающих требованиям информационной безопасности;

- установлению полномочий пользователей и форм представления информации пользователям Информационных систем;

- организации работы с персоналом, включая ознакомление с кандидатами, их изучение и проверку, обучение персонала требованиям информационной безопасности;

- осуществлению контроля эффективности организационных мер защиты.

8.5. Программно-технические меры защиты планируются и проводятся в соответствии с требованиями законодательства Российской Федерации.

9. Обязанности структурных подразделений по обеспечению информационной безопасности

9.1. Непосредственно ответственным в Учреждении за обеспечение информационной безопасности является подразделение по информационной безопасности – отдел информационной безопасности, которое в рамках своих полномочий отвечает за организацию и проведение в Учреждении, организацию и проведение мероприятий по обеспечению защиты информации от технических разведок и утечки по техническим каналам.

9.2. Подразделение по информационной безопасности обязано:

- организовывать и координировать работы по защите информации в Учреждении;

- осуществлять планирование работ по защите информации от иностранных технических разведок и от ее утечки по техническим каналам;

- организовывать аттестацию подведомственных объектов по выполнению требований обеспечения защиты информации при проведении работ со сведениями ограниченного доступа, контролировать выполнение требований аттестатов соответствия;

- организовывать в установленном порядке расследования причин и условий появления нарушений по вопросам защиты информации и разрабатывать предложения по устранению недостатков и предупреждению подобного рода нарушений, а также осуществлять контроль за устранением этих нарушений;

- разрабатывать предложения по организации и совершенствованию системы защиты информации, в том числе по вопросам, решаемым в рамках областных программ;

- организовывать и координировать разработку, внедрение и эксплуатацию системы мер по безопасности информации, обрабатываемой техническими средствами, в целях предотвращения утечки информации по техническим каналам;

- организовывать разработку комплекса мероприятий по защите информации при установлении и осуществлении научно-технических и торгово-экономических связей с

зарубежными фирмами, а также при посещении иностранными представителями подведомственных предприятий, учреждений и организаций;

- организовывать и проводить занятия с пользователями Информационных систем по вопросам защиты информации.

9.3. Подразделение по информационной безопасности наделяется правом:

- требовать от всех структурных подразделений и пользователей соблюдения условий информационной безопасности, предоставления подробной информации, необходимой для осуществления своих функций;

- осуществлять проверку состояния любых систем, проектов, системных и информационных ресурсов и технологий, приостанавливать либо ограничивать их функционирование в случаях нарушения требований информационной безопасности;

- вносить предложения руководству о прекращении либо изменении режима функционирования указанных систем и технологий, а также о санкциях в отношении должностных лиц, действия которых подвергают риску информационную безопасность.

9.4. Стратегические и тактические задачи создания, модернизации и развития информационных систем, архитектуры безопасности и защитных механизмов включаются в перспективные, годовые или в тематические планы Учреждения, согласовываются с заинтересованными подразделениями и утверждаются руководством.

10. Контроль выполнения положений настоящей Политики

Сотрудники, использующие ресурсы локальной вычислительной сети или сети международного информационного обмена, должны осознавать, что любая их деятельность в сетях не защищена от просмотра третьими лицами.

Если информация не является общедоступной, сотрудник не должен передавать информацию по каналам Интернет/Интранет без применения соответствующих мер защиты.

Подразделение по информационной безопасности (ответственный специалист) Учреждения сохраняет за собой право в любое время и без предварительного предупреждения исследовать электронную почту, персональные каталоги и другую информацию на компьютерах сотрудников с целью проверки выполнения сотрудником настоящей Политики.

Сотрудники Учреждения не имеют права перехватывать, просматривать электронную информацию других пользователей или способствовать этому. Учреждение обязуется соблюдать права сотрудников, включая право на защиту личной информации, а также обязуется обеспечивать защиту внутренних ресурсов корпоративной локальной вычислительной сети. Для выполнения этой задачи возможно применение механизмов перехвата и контролирования содержимого электронной информации.

Работники Учреждения должны сознавать, что каналы электронной связи не шифруются по умолчанию.

Шифрование должно использоваться для защиты паролей доступа и другой информации, которая может быть использована для доступа к ресурсам и сервисам, размещенной в незащищенной зоне или передающейся по каналам связи (например, Интернет) в открытом виде.

Шифрование любой другой информации должно быть согласовано с подразделением (специалистом) по информационной безопасности. В случае применения шифрования должны использоваться только утвержденные алгоритмы и инструменты. Запрещается использовать не сертифицированные и (или) не рекомендованные Федеральной службой безопасности Российской Федерации средства шифрования.

Для подтверждения достоверности сообщений (почтовых и иных) рекомендовано использовать сертифицированные средства электронной подписи (ЭП).

Электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.