Приложение №1
к приказу от «14» марта 2018.
№ 27-ОД

Политика информационной безопасности в Муниципальном бюджетном дошкольном образовательном учреждении – детском саду №4 города Агрыз Агрызского муниципального района Республики Татарстан

1. Общие положения

1.1. Политика информационной безопасности (далее – Политика ИБ) в Муниципальном бюджетном дошкольном образовательном учреждении – детском саду №4 города Агрыз Агрызского муниципального района Республики Татарстан (далее – ДОУ) определяет цели и задачи системы обеспечения информационной безопасности и устанавливает совокупность правил, требований и руководящих принципов в области информационной безопасности, которыми руководствуется МКУ «Управление образования» в своей деятельности.

1.2. Политика ИБ учитывает современное состояние и ближайшие перспективы развития информационных технологий в ДОУ, цели, задачи и правовые основы их эксплуатации, режимы функционирования, а также содержит анализ угроз безопасности для объектов и субъектов информационных отношений ДОУ.

1.3. Обеспечение информационной безопасности включает в себя любую деятельность, направленную на защиту информации.

1.4. Информационная безопасность ДОУ заключается в неукоснительном соблюдении всеми сотрудниками ДОУ требований и принципов, изложенных в Политике ИБ.

1.5. Разработка Политики ИБ, внесение изменений и общий контроль выполнения требований по обеспечению информационной безопасности ДОУ осуществляется администрацией ДОУ.

1.6. Политика ИБ является методологической основой для обеспечения режима информационной безопасности ДОУ, служит руководством при разработке соответствующих положений, правил, инструкций.

1.7. Все сотрудники ДОУ, ответственны за обеспечение выполнения требований информационной безопасности, определяемых в настоящей Политике ИБ.

1.8. Политика ИБ разработана на основе нормативных и распорядительных документов в области информационной безопасности Российской Федерации.

1.9. Политика ИБ является документом, доступным каждому сотруднику ДОУ.

1.10. Документами, детализирующими положения Политики ИБ применительно к одной или нескольким областям информационной безопасности, видам и технологиям деятельности ДОУ являются частные политики по обеспечению информационной безопасности, инструкции, методические пособия и рекомендации, которые являются документами по информационной безопасности второго уровня .

2. Объекты информационной безопасности

2.1. Основными объектами информационной безопасности в ДОУ являются:

- информационная инфраструктура, включающая технические и программно-аппаратные комплексы, информационные системы, системы и средства защиты информации, системы и(или) подсистемы обработки и анализа информации средства обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, объекты и помещения, в которых размещены такие системы.

- информационные ресурсы с ограниченным доступом, составляющие государственную тайну, персональные данные, сведения ограниченного распространения или иные чувствительные к случайным и несанкционированным воздействиям и нарушению их безопасности информационные ресурсы, а также открыто распространяемая информация, необходимая для работы ДОУ, независимо от формы и вида ее представления;

- процессы обработки информации в ЕСС ДОУ, информационные технологии, регламенты и процедуры ввода, сбора, обработки, хранения и передачи информации;

- персонал разработчиков, пользователей систем и обеспечивающий ее стабильное функционирование;

2.2. Информационная среда ДОУ, локально-вычислительные сети разного уровня и комплексы автоматизированных рабочих мест, объединенных в единую структурированную сеть.

2.3. К основным особенностям информационной среды ДОУ относятся:

- объединение в единые системы разнообразных технических и программно-аппаратных средств обработки и передачи информации;

- расширение сферы использования информационных систем ДОУ;

- объединение в единую информационную среду различных неоднородных моделей информационных систем.

- разнообразие решаемых задач и типов обрабатываемых данных, сложные режимы автоматизированной обработки информации;

- важность и ответственность решений, принимаемых на основе автоматизированной обработки информации;

- объединение в единых базах данных информации различного назначения, принадлежности и уровней конфиденциальности;

- необходимость обеспечения непрерывности функционирования ДОУ;

- разнообразие, значимость и интенсивность информационных потоков;

- разнообразие категорий пользователей, разработчиков и обеспечивающего персонала информационных систем.

2.4. Защите подлежит вся информация и информационные ресурсы, циркулирующие в ДОУ, независимо от ее представления и местонахождения в ЕСС ДОУ.

3. Цели и задачи деятельности по обеспечению информационной безопасности

3.1 Основной целью деятельности по обеспечению информационной безопасности ДОУ является защита объектов информационной ДОУ от возможного нанесения материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на информацию, ее носителей, процессы обработки и передачи, а также минимизация уровня информационной безопасности других угроз.

3.2 Основными задачами деятельности по обеспечению информационной безопасности являются:

- Своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба, нарушению нормального функционирования объектов информационной безопасности ДОУ;

- Создание механизма оперативного реагирования на угрозы безопасности информации и негативные тенденции;

- Создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидации последствий нарушения безопасности информации;

- Защита от вмешательств посторонних лиц в процесс функционирования объектов информационной безопасности ДОУ;

- Разграничение доступа пользователей к объектам информационной безопасности и иным ресурсам ДОУ;
- Обеспечение аутентификации пользователей, участвующих в информационном обмене;
- Защита от несанкционированной модификации используемых в ЕСС ДОУ программных средств, а также защиту от внедрения несанкционированных программ, включая компьютерные вирусы;
- Защиту информации ограниченного пользования от утечки по техническим каналам при ее обработке, хранении и передачи по каналам связи;
- Обеспечение бесперебойного функционирования криптографических средств защиты информации.

3.3 Поставленная цель защиты и решение перечисленных задач достигаются:
- Учетом всех подлежащих защите объектов информационной безопасности ДОУ;
- Регистрацией в журналах действий персонала, осуществляющего обслуживание и модификацию объектов информационной безопасности
- Полнотой, реальной выполнимостью и непротиворечивостью требований организационно – распорядительных документов ДОУ по вопросам обеспечения безопасности информации;
- Подготовкой должностных лиц, ответственных за организацию и осуществлению практических мероприятий по обеспечению безопасности информации и процессов ее обработки;
- Наделением каждого пользователя оптимально-необходимыми для выполнения им своих функциональных обязанностей полномочиями по доступу к информационным ресурсам ДОУ;
- Четким знанием и строгим соблюдением всеми пользователями объектов информационной безопасности ДОУ требований организационно – распорядительных документов по вопросам обеспечения безопасности информации;
- Персональной ответственностью за свои действия каждого сотрудника, в рамках своих функциональных обязанностей имеющего доступ к объектов информационной безопасности ДОУ;
- Применением физических и технических средств защиты объектов информационной безопасности ДОУ и непрерывной административной поддержкой их использования
- Эффективным контролем над соблюдением пользователями информационных ресурсов ДОУ требований по обеспечению безопасности информации;

4. Основные угрозы безопасности информации в ДОУ.

4.1 Под угрозами безопасности информации в ДОУ понимается потенциально возможные негативные воздействия на защищаемую информацию.

4.2 Основными источниками угроз безопасности информации в ДОУ являются:
- Непреднамеренные, т.е. действия, вызванные некомпетентностью или халатностью пользователей (персонала);
- Преднамеренные, т.е. действия, вызванные злым умыслом, независимо от того, внешним или внутренним относительно объектов информационной безопасности ДОУ является источник угрозы;
- Ошибки, допущенные при разработке компонентов объектов информационной безопасности ДОУ и их систем защиты, ошибки в программном обеспечении, отказы и сбои технических средств;
- Аварии, стихийные бедствия.

4.3 Сотрудники ДОУ, зарегистрированные как легальные пользователи ЕСС ДОУ или обслуживающие ее компоненты, являются внутренними источниками случайных

воздействия, т.к. имеют непосредственный доступ к процессам обработки информации и могут совершать непреднамеренные ошибки и нарушения действующих правил, инструкций, регламентов;

4.4 Возможные пути реализации непреднамеренных угроз безопасности ДОУ:

- Неумышленные действия, приводящие к частичному или полному нарушению функциональности компонентов объектов информационной ДОУ или разрушению информационных или программно – технических ресурсов;
- Неосторожные действий, приводящие к разглашению информации ограниченного распространения;
- Разглашение, передача или утрата атрибутов разграничения доступа;
- Игнорирование организационных ограничений при работе с информационными ресурсами;
- Проектирование архитектуры систем, технологий обработки данных с возможностями, представляющими опасность для функционирования объектов информационной безопасности ДОУ и безопасности информации;
- Пересылка данных по ошибочному адресу (устройству);
- Ввод ошибочных данных;
- Неумышленная порча носителей информации;
- Неумышленное повреждение каналов связи;
- Неправомерное отключение оборудования или изменение режимов работы устройств или программ;
- Заражение компьютеров вирусами;
- Несанкционированные запуск технологических программ, способных вызвать потерю работоспособности компонентов информационных систем или осуществляющих в них необратимые изменения;
- Некомпетентное использование, настройка или неправомерное отключение средств защиты.

4.5 Возможные пути реализации преднамеренных угроз безопасности ДОУ:

- Умышленные действия, приводящие к частичному или полному нарушению функциональных компонентов объектов информационной безопасности ДОУ или разрушению информационных или программно – технических ресурсов;
- Действия по дезорганизации функционирования объектов информационной безопасностиДОУ;; хищение документов и носителей информации;
- Несанкционированное копирование документов и носителей информации; умышленное искажение информации. Ввод неверных данных;
- Отключение или ввод из строя подсистем обеспечения функционирования объектов информационной безопасности ДОУ;
- Перехват данных, передаваемых по каналам связи и их анализ;
- Хищение производственных отходов;
- Незаконное получение атрибутов разграничения доступа;
- Несанкционированный доступ к объектов информационной безопасности ДОУ с рабочих станций легальных пользователей;
- Хищение или вскрытие шифров криптозащиты информации;
- Внедрение аппаратных или программных закладок с целью скрытно осуществлять доступ к информационным ресурсам или дезорганизации функционирования компонентов объектов информационной безопасности ДОУ;
- Незаконное использование оборудования, программных средств или информационных ресурсов.

4.6 Возможные пути реализации основных естественных угроз безопасности ДОУ:

- Выход из строя оборудования объектов информационной безопасности и оборудования обеспечения их функционирование;
- Выход из строя или невозможность использования линий связи;

- Пожары, наводнения и другие стихийные бедствия.

4.7 Нарушитель – лицо, которое предприняло попутку выполнения запрещенных действий по ошибке, незнанию или осознанно со злым умыслом или без такового и использующее для этого различные возможности, методы и средства.

4.8 Злоумышленник – нарушитель, действующий намеренно из корыстных, идейных или иных побуждений.

4.9 Система обеспечения информационной безопасности ДОУ должна строиться исходя из предположений о возможных типах нарушителей и злоумышленников в системе.

4.10 Некомпетентный пользователь – сотрудник ДОУ использующий только штатные средства,, который может предпринимать попытки выполнения запрещенных действий, доступа к защищаемым объектов информационной безопасности ДОУ с превышением своих полномочий, ввода некорректных данных, нарушения правил и регламентов работы с информацией и т.д.

4.11 Любитель – сотрудник ДОУ, пытающийся нарушить систему защиты без корыстных целей или злого умысла. Для преодоления системы защиты и совершения запрещенных действий он может использовать различные методы получения дополнительных полномочий доступа к ресурсам, недостатки в построение системы защиты и доступные ему штатные средства. Помимо этого он может попытаться использовать дополнительные нештатные инструментальные и технологические программные средства, самостоятельно разработанные программы или стандартные дополнительные технические средства.

4.12 Внутренний злоумышленник – сотрудник ДОУ, действующий целенаправленно из корыстных интересов. Может использовать весь набор методов и средств взлома системы защиты, включая агентурные методы, пассивные средства, методы и средства активного воздействия, а также комбинации воздействий, как изнутри, так и извне ДОУ.

4.13 Внешний злоумышленник – постороннее лицо, действующее целенаправленно из корыстных интересов. Может использовать весь набор методов и средств взлома системы защиты, включая агентурные методы, пассивные средства, методы и средства активного воздействия, а также комбинации воздействий, как изнутри, так и извне ДОУ.

4.14 К внутренним нарушителем могут быть отнесены лица из следующих категорий сотрудников ДОУ:

- Зарегистрированные пользователи ЕСС ДОУ;
- Сотрудники ДОУ, не являющиеся зарегистрированными пользователями и не допущенные к ресурсам ЕСС, но имеющие доступ в здание и помещения;
- Персонал, обеспечивающий обслуживание технические средства объектов информационной безопасности ДОУ..
- Специалисты, задействованные в сопровождении программного обеспечения;

4.15 Внешним нарушителем может быть лицо из следующих категорий:

- Уволенные сотрудники ДОУ;
- Представители организаций, взаимодействующих по вопросам технического обеспечения ДОУ;
- Посетители;
- Члены преступных организаций;
- Лица, случайно или умышленно проникшие в ЕСС ДОУ из внешних телекоммуникационных сетей (хакеры).

5. Основные принципы построения системы информационной безопасности ДОУ.

5.1 Законность.

Предполагает осуществление защитных мероприятий и разработку систем безопасности информации ДОУ в соответствии с действующим законодательством в области информационных технологий. Все пользователи объектов информационной безопасности ДОУ должны иметь представление об ответственности за правонарушения в области информационных технологий. Реализация данного принципа необходима для защиты имени и репутации ДОУ.

5.2 Системность.

Предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности объектов информационной безопасности ДОУ. При создании системы защиты должны учитываться все слабые и наиболее уязвимые места объектов информационной безопасности ДОУ. Система защиты должна строиться с учетом всех известных каналов проникновения и несанкционированного доступа к информации и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

5.3 Компетентность.

Предполагает применение разнородных средств защиты при построении целостной системы защиты, перекрывающей все значимые каналы реализации угроз и не содержащей слабых мест на стыках ее отдельных компонентов. Защита должна строиться эшелонировано..

5.4 Непрерывность и целостность защиты.

Это процесс, осуществляемый руководством ДОУ, который должен постоянно идти на всех уровнях внутри ДОУ. Каждый сотрудник ДОУ должен принимать участие в этом процессе. Деятельность по обеспечению информационной безопасности является составной частью повседневной деятельности ДОУ.

5.5 Своевременность.

Носит упреждающий характер мер обеспечения безопасности информации. Разработка системы защиты должна вестись параллельно с разработкой и развитием самой защищаемой системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, создать более эффективные системы, обладающие достаточными компетенциями.

5.6 Преемственность и совершенствование.

Предполагает постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования объектов информационной безопасности ДОУ и системы ее защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в области информационных технологий.

5.7 Разумная достаточность.

Предполагает соответствие уровня затрат на обеспечение безопасности информации к величине возможного ущерба. Создать абсолютно непреодолимую систему защиты принципиально невозможно. Пока информация находится в обращении, принимаемые меры могут только снизить вероятность негативных воздействий, но не исключить их полностью. При достаточном количестве времени и средств – возможно, преодолеть любую защиту. Поэтому имеет смысл рассматривать некоторый приемлемый уровень обеспечения безопасности.

5.8 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 строиться таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.

5.9 Оптимизация полномочий.

Предполагает предоставление пользователям оптимальных прав доступа в соответствии со служебной необходимостью. Доступ к информации должен предоставляться только в том случае и объеме, когда это необходимо сотруднику для выполнения его должностных обязанностей.

5.10 Исключение конфликта интересов.

Предполагает четкое разделение обязанностей сотрудников и исключение ситуаций, когда сфера ответственности сотрудников допускает конфликт интересов. Сферы потенциальных конфликтов должны выявляться, минимизироваться, и находиться под строгим независимым контролем. Реализация данного принципа предполагает, что не один сотрудник не должен иметь полномочий, позволяющих ему единолично осуществлять выполнение критичных операций.

5.11 Взаимодействие и сотрудничество.

Предполагает создание благоприятной атмосферы в коллективах структурных подразделений. В такой обстановке сотрудники должны осознанно соблюдать установленные правила. Все сотрудники ДОУ должны понимать свою роль в процессе обеспечения информационной безопасности и принимать в этом участие в этом процессе.

5.12 Гибкость системы защиты.

Предполагает способность системы обеспечения информационной безопасности реагировать на изменения внешней среды и условий осуществления ДОУ своей деятельности.

5.13 Простота применения средств защиты.

Предполагает интуитивно понятные и простые в использовании механизмы и методы защиты. 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.

5.14 Обоснованность и техническая реализуемость.

Предполагает реализацию на современном уровне развития науки и техники информационных технологий, технических и программных средств, а также средств и мер защиты информации.

5.15 Специализация и профессионализм.

Предполагает привлечение к разработке средств и реализации мер защиты информации специализированных организаций, лицензированных на осуществление деятельности по обеспечению безопасности информационных ресурсов, имеющих практический опыт работы и государственную лицензию на право оказания услуг в этой области. Реализация административных мер и эксплуатация средств защиты должна осуществляться профессионально подготовленными ДОУ.

5.16 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 деятельность любого пользователя, каждого средства защиты и в отношении любого объекта защиты должен осуществляться на основе применения средств оперативного контроля и регистрации и должен охватывать как несанкционированные, так и санкционированные действия пользователей. Вместе с тем, эффективная система обеспечения информационной безопасности требует наличия адекватной и всеобъемлющей информации о текущем состоянии процессов, связанных с движением информации и сведений о соблюдении установленных нормативных требований, а также дополнительной информации, имеющей отношение к принятию решений.

5.17 Недостатки системы обеспечения информационной безопасности, выявленные сотрудниками ДОУ должны немедленно доводиться до сведения руководителя ДОУ и оперативно устраняться.

6. Меры, методы и средства обеспечения требуемого уровня защищенности информационных ресурсов.

Предполагается, что несанкционированный доступ на объекты информационной безопасности посторонних лиц исключается мерами физической защиты.

6.1 Все меры обеспечения безопасности информационной системы ДОУ подразделяются на следующие виды:

- правовые;
- морально – этические;
- технологические;
- организационные;
- физические;
- технические.

6.2 Правовые.

К данному виду мер защиты относятся действующие законы, указы, нормативные акты, соглашения, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных взаимодействий в процессе обработки и использовании, а также устанавливающие ответственность за нарушения этих правил.

Данные меры носят в основном упреждающие характер и требуют постоянной разъяснительной работы с пользователями.

6.3 Морально – этические.

К данному виду мер защиты относятся нормы поведения, которые традиционно сложились или складываются по мере распространения информационных технологий в обществе.

Данные меры большей частью не являются обязательными, однако, их несоблюдение может привести к серьезным потерям информации и непредсказуемым последствиям.

6.4 Технологические.

К данному виду мер защиты относятся разного рода технологические решения и приемы, направленные на уменьшение возможности совершения сотрудниками ДОУ ошибок и нарушений в рамках предоставленных им прав и полномочий.

6.5 Организационные.

К данному виду мер защиты относятся меры организационного характера, регламентирующие процессы функционирования системы обработки данных, использование ее ресурсов, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности.

Главной целью организационных мер, предпринимаемых на высшем управленческом уровне – сформировать политику в области обеспечения безопасности информации и обеспечить ее выполнение, выделяя необходимые технические, финансовые и человеческие ресурсы, а так же постоянно контролируя состояние дел.

6.6 Уровни политики обеспечения безопасности информации

Политика в области обеспечения безопасности информации в ДОУ разделена на два уровня:

- верхний;
- нижний.

К верхнему уровню политики обеспечения безопасности информации относятся решения руководства, затрагивающие деятельность ДОУ в целом. На данном уровне четко определяется сфера влияние и ограничения при определении целей безопасности информации, определяются ресурсы, с помощью которых они будут достигнуты. Находится компромисс между приемлемым уровнем безопасности и функциональностью.

На нижнем уровне политики обеспечения безопасности информации определяются процедуры и правила достижения целей и решений задач безопасности информации.

6.7 Доступ пользователей к работе с объектами информационной безопасности ДОУ и доступ к их ресурсам должен быть строго регламентирован. Любые изменения состава и полномочий пользователей должны производиться установленным порядком, согласно регламента предоставления доступа пользователей.

6.8 Все сотрудники ДОУ, зарегистрированные как легальные пользователи ЕСС ДОУ должны нести персональную ответственность за нарушения установленного порядка обработки информации, правил хранения, использования и передачи, находящихся в их распоряжении защищаемых ресурсов системы.

6.9 Подлежащие защите ресурсы системы подлежат строгому учету.

6.10 Все неиспользуемые в работе устройства ввода – вывода информации на рабочих местах сотрудников, работающих с конфиденциальной информацией, должны быть по возможности отключены, не нужные для работы программные средства и данные с дисков также должны быть удалены.

6.11 В компонентах объектов информационной безопасности ДОУ и на рабочих местах пользователей должны устанавливаться и использоваться только лицензионные программные средства, прошедшие антивирусную проверку. Использование программного обеспечения, не прошедшего проверку и не учтенного в ДОУ, должно быть запрещено.

6.12 Пользователи объектов информационной безопасности ДОУ должны быть ознакомлены со своим уровнем полномочий, а также организационной – распорядительной, нормативной, технической и эксплуатационной документацией, определяющей требования и порядок обработки информации в ДОУ.

6.13. Для непосредственной организации и эффективного функционирования системы обеспечения информационной безопасности, исключающей возможные конфликты интересов, в ДОУ целесообразно ввести сектор по обеспечение информационной безопасности, с утверждением необходимой штатной численности специалистов, и возложением на них соответствующих функций и задач.

6.14 Любое грубое нарушение порядка и правил пользования информационными ресурсами ДОУ должно расследоваться. К виновным применяться адекватные меры воздействия.

6.15 Для реализации принципа персональной ответственности пользователей за свои действия необходимы:

- Индивидуальная идентификация пользователей и инициированных им процессов;
- Проверка подлинности пользователей на основе паролей, ключей на различной основе и т.д.;
- Реакция на попытке несанкционированного доступа (сигнализация, блокировка и т.д.)

6.16 Для обеспечения информационной безопасности ДОУ используются следующие средства защиты:

- физические;
- технические;
- средства идентификации и аутентификации пользователей;
- средства разграничения доступа;
- средства обеспечения контроля и целостности;

- средства оперативного контроля и регистрации событий безопасности,
- криптографические средства.

6.17 Технические меры защиты.

Основаны на использовании различных электронных устройств и специальных программ и выполняющих функции защиты.

6.18 средства разграничения доступа

В целях предотвращения работы с объектами информационной безопасности ДОУ посторонних лиц, необходимо обеспечить возможность распознавания каждого легального пользователя.

6.19 Средства идентификации и аутентификации пользователей

Зоны ответственности и задачи конкретных технических средств защиты устанавливаются исходя из их возможностей и эксплуатационных характеристик, описанных в документации на данные средства.

6.20 Средства обеспечения целостности

Средства обеспечения целостности включают в свой состав средства резервного копирования, программы антивирусной защиты, программы восстановления целостности операционной среды и баз данных.

6.21 средства оперативного контроля и регистрации событий безопасности

Средства контроля целостности информационных объектов информационной безопасности ДОУ предназначены для своевременного обнаружения модификации или искажения ресурсов системы. Они позволяют обеспечивать правильность функционирования системы защиты и целостность хранимой и обрабатываемой информации.

Средства объективного контроля должны обеспечивать обнаружение и регистрацию всех событий, которые могут повлечь за собой нарушение Концепции ИБ и привести к возникновению кризисных ситуаций.

При регистрации событий безопасности в журнале должна фиксироваться следующая информация:

- дата и время события,
- идентификатор субъекта, осуществляющий регистрируемое действие;
- действие.

6.22 криптографические средства

Все средства криптографической защиты информации в ДОУ должны строиться на основе базисного криптографического ядра, прошедшего всесторонние исследования специализированными организациями.

6.23 Управление системой обеспечения безопасности информации представляет собой целенаправленное воздействие на компоненты системы обеспечения безопасности с целью достижения требуемых показателей и норм защищенности объектов информационной безопасности ДОУ в условиях реализации основных угроз безопасности.

6.24 Контроль эффективности защиты

Контроль эффективности защиты информации осуществляется с целью своевременного выявления и предотвращения угроз безопасности. Контроль может производиться как ответственным сотрудником за информационную безопасностьДОУ, так и привлекаемыми для этой цели организациями, имеющими лицензию на этот вид деятельности.

7. Порядок утверждения, внесения изменений и дополнений

7.1 Настоящая Политика ИБ вступает в законную силу с даты утверждения.

7.2 Изменения и дополнения в настоящую Политику вносятся по инициативе руководства ДОУ ответственного специалиста.

7.3 Пересмотр Политики ИБ производится не реже 1 раза в год.

7.4 В случае вступления отдельных пунктов в противоречие с новыми законодательными актами в сфере информационных технологий - эти пункты данной концепции утрачивают юридическую силу до момента внесения изменений в настоящую Политику ИБ.

Требования Политики ИБ могут развиваться другими внутренними документами ДОУ.