Приложение № 1
к приказу по МБДОУ № 6
от 27.12.2024 № 93-ОД

ПОЛИТИКА
МБДОУ № 6 в отношении обработки информации и персональных данных

1. Термины и определения

Персональные данные (ПДн) - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн).

Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку ПДн, а также определяющие цели обработки ПДн, состав ПДн, подлежащих обработке, действия (операции), совершаемые с ПДн.

Обработка ПДн - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПДн, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн.

Автоматизированная обработка ПДн - обработка ПДн с помощью средств вычислительной техники.

Распространение ПДн - действия, направленные на раскрытие ПДн неопределенному кругу лиц.

Предоставление ПДн - действия, направленные на раскрытие ПДн определенному лицу или определенному кругу лиц.

Блокирование ПДн - временное прекращение обработки ПДн (за исключением случаев, если обработка необходима для уточнения ПДн).

Уничтожение ПДн - действия, в результате которых становится невозможным восстановить содержание ПДн в ИСПДн и (или) в результате которых уничтожаются материальные носители ПДн.

Обезличивание ПДн - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту ПДн.

Трансграничная передача ПДн - передача ПДн на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

2. Назначение и правовая основа документа

Политика **МБДОУ № 6** (далее по тексту – Политика) определяет систему взглядов на проблему обеспечения безопасности ПДн и представляет собой систематизированное изложение целей и задач защиты, как одно или несколько правил, процедур, практических приемов и руководящих принципов в области информационной безопасности, которыми руководствуется **МБДОУ № 6** в своей

деятельности, а также основных принципов построения, организационных, технологических и процедурных аспектов обеспечения безопасности информации.

Законодательной основой настоящей Политики являются Конституция Российской Федерации, Гражданский, Уголовный кодексы, Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральный закон РФ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации», законы, указы, постановления, другие нормативные документы действующего законодательства Российской Федерации, документы ФСТЭК и ФСБ России.

Использование данной Политики в качестве основы для построения комплексной системы информационной безопасности информации **МБДОУ № 6** позволит оптимизировать затраты на ее построение.

При разработке Политики учитывались основные принципы создания комплексных систем обеспечения безопасности информации, характеристики и возможности организационно-технических методов и современных аппаратно-программных средств защиты и противодействия угрозам безопасности информации.

Основные положения Политики базируются на качественном осмыслении вопросов безопасности информации и не затрагивают вопросов экономического (количественного) анализа рисков и обоснования необходимых затрат на защиту информации.

3. Основными объектами системы безопасности информации в **МБДОУ № 6** являются:

– информационные ресурсы с ограниченным доступом, содержащие ПДн и сопутствующую информацию, не составляющую государственную тайну, в том числе о родившихся и зарегистрированных по месту жительства обучающихся, а также сведения обо всех этапах обучения детей;

– процессы обработки информации в информационных системах **МБДОУ № 6**, информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации, персонал пользователей системы и ее обслуживающий персонал;

– 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 расположены технические средства обработки информации.

4. Интересы затрагиваемых субъектов информационных отношений

Субъектами информационных отношений при обеспечении безопасности информации МБДОУ № 6 являются:

– МБДОУ № 6, как собственник информационных ресурсов и технических средств обработка информации;

– Субъекты персональных данных, в том числе родившиеся и зарегистрированные по месту жительства (обучающиеся).

– 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 информационных систем посторонних лиц (доступ к информационным ресурсам должны иметь только зарегистрированные в установленном порядке пользователи);

– разграничение доступа пользователей к информационным, аппаратным, программным и иным ресурсам **МБДОУ № 6** (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям для выполнения своих служебных обязанностей), то есть защиту от несанкционированного доступа;

– обеспечение аутентификации пользователей, участвующих в информационном обмене (подтверждение подлинности отправителя и получателя информации);

– защиту от несанкционированной модификации используемых в информационных системах **МБДОУ № 6** 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.

4.3. Основные пути решения задач системы защиты

Поставленные основные цели защиты и решение перечисленных выше задач достигаются:

– строгим учетом всех подлежащих защите ресурсов информационных систем **МБДОУ № 6** (информации, задач, документов, каналов связи, серверов, автоматизированных рабочих мест);

– журналированием действий персонала, осуществляющего обслуживание и модификацию программных и технических средств информационных систем;

– полнотой, реальной выполнимостью и непротиворечивостью требований организационно-распорядительных документов **МБДОУ № 6** по вопросам обеспечения безопасности информации;

– подготовкой должностных лиц (сотрудников), ответственных за организацию и осуществление практических мероприятий по обеспечению безопасности ПДн и процессов их обработки;

– наделением каждого сотрудника (пользователя) минимально необходимыми для выполнения им своих функциональных обязанностей полномочиями по доступу к информационным ресурсам **МБДОУ № 6**;

– четким знанием и строгим соблюдением всеми пользователями информационных систем **МБДОУ № 6** требований организационно-распорядительных документов по вопросам обеспечения безопасности информации;

– персональной ответственностью за свои действия каждого сотрудника, в рамках своих функциональных обязанностей имеющего доступ к информационным ресурсам **МБДОУ № 6**;

– непрерывным поддержанием необходимого уровня защищенности элементов информационной среды;

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

– эффективным контролем над соблюдением пользователями информационных ресурсов требований по обеспечению безопасности информации;

– юридической защитой интересов МБДОУ № 6 при взаимодействии 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.

5. Построение системы, обеспечение безопасности информации **МБДОУ № 6** и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

5.1. Законность

Предполагает осуществление защитных мероприятий и разработку системы безопасности информации **МБДОУ № 6** в соответствии с действующим законодательством в области защиты информации, а также других законодательных актов по безопасности информации РФ, с применением всех дозволенных методов обнаружения и пресечения правонарушений при работе с информацией. Принятые меры безопасности ПДн не должны препятствовать доступу правоохранительных органов в предусмотренных законодательством случаях.

Все пользователи информационных систем должны иметь представление об ответственности за правонарушения в области защиты информации.

5.2. Системность

Системный подход к построению системы защиты информации в **МБДОУ № 6** предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности информации.

При создании системы защиты должны учитываться все слабые и наиболее уязвимые места информационных систем, а также характер, возможные объекты и направления атак на нее со стороны нарушителей (особенно высококвалифицированных злоумышленников).

Система защиты должна строиться с учетом не только всех известных каналов проникновения и несанкционированного доступа к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

5.3. 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 эшелонировано. Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами.

5.4. Непрерывность защиты

Обеспечение безопасности информации - процесс, осуществляемый руководством **МБДОУ № 6**, администратором безопасности информации и сотрудниками всех уровней. 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 внутри **МБДОУ № 6** и каждый сотрудник должен принимать участие в этом процессе. Деятельность по обеспечению информационной безопасности является составной частью повседневной деятельности **МБДОУ № 6** И ее эффективность зависит от участия руководства **МБДОУ № 6** в обеспечении информационной безопасности информации.

Кроме того, большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, переопределение полномочий и т.п.). Перерывы в работе средств защиты могут быть использованы злоумышленниками для анализа применяемых методов и средств защиты, для внедрения специальных программных и аппаратных "закладок" и других средств преодоления защиты.

5.5. Своевременность

Предполагает упреждающий характер мер обеспечения безопасности информации, то есть постановку задач по комплексной защите информации и реализацию мер обеспечения безопасности информации на ранних стадиях разработки информационных систем в целом и их систем защиты, в частности.

Разработка системы защиты должна вестись параллельно с разработкой и развитием самих защищаемых информационных систем. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, создать более эффективные (как по затратам ресурсов, так и по стойкости) системы, обладающие достаточным уровнем защищенности.

5.6. Преемственность и совершенствование

Предполагает постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования информационных систем МБДОУ № 6 и системы их защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.

5.7. Разумная достаточность (экономическая целесообразность)

Предполагает соответствие уровня затрат на обеспечение безопасности информации ценности информационных ресурсов и величине возможного ущерба от их разглашения, утраты, утечки, уничтожения и искажения. Используемые меры

Предполагает создание благоприятной атмосферы в коллективе **МБДОУ № 6** В такой обстановке сотрудники должны осознанно соблюдать установленные правила и оказывать содействие деятельности администратора безопасности информации.

Важным элементом эффективной системы обеспечения безопасности информации в МБДОУ № 6 является высокая культура работы с информацией. Руководство МБДОУ № 6 несет ответственность за строгое соблюдение этических норм и стандартов профессиональной деятельности, подчеркивающей и демонстрирующей персоналу на всех уровнях важность обеспечения информационной безопасности МБДОУ № 6. Все сотрудники МБДОУ № 6 должны понимать свою роль в процессе обеспечения информационной безопасности и принимать участие в этом процессе. Несмотря на то, что высокая культура обеспечения информационной безопасности не гарантирует автоматического достижения целей, ее отсутствие создает больше возможностей для нарушения безопасности или не обнаружения фактов ее нарушения.

5.12. Гибкость системы защиты

Система обеспечения информационной безопасности должна быть способна реагировать на изменения внешней среды и условий осуществления Управлением своей деятельности. В число таких изменений входят:

– изменения организационной и штатной структуры **МБДОУ № 6**

– изменение существующих или внедрение принципиально новых информационных систем;

– новые технические средства.

Свойство гибкости системы обеспечения информационной безопасности избавляет в таких ситуациях от необходимости принятия кардинальных мер по полной замене средств и методов защиты на новые, что снижает ее общую стоимость.

5.13. Открытость алгоритмов и механизмов защиты

Суть принципа открытости алгоритмов и механизмов защиты состоит в том, что защита не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты не должно давать возможности ее преодоления (даже авторам). Это, однако, не означает, что информация об используемых системах и механизмах защиты должна быть общедоступна.

5.14. 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.

5.15. Обоснованность и техническая реализуемость

Информационные технологии, технические и программные средства, средства и меры защиты информации должны быть реализованы на современном уровне

профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом информационных систем **МБДОУ № 6**.

6.2. Морально-этические меры защиты

К морально-этическим мерам относятся нормы поведения, которые традиционно сложились или складываются по мере распространения информационных технологий в обществе. Эти нормы большей частью не являются обязательными, как законодательно утвержденные нормативные акты, однако, их несоблюдение может привести к падению авторитета, престижа человека, группы лиц или **МБДОУ № 6** в целом. Морально-этические нормы бывают как неписаные, так и писаные, то есть оформленные в некоторый свод (устав) правил или предписаний. Морально этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в коллективе.

6.3. Технологические меры защиты

К данному виду мер защиты относятся разного рода технологические решения и приемы, основанные на использовании некоторых видов избыточности (структурной, функциональной, информационной, временной и т.п.) и направленные на уменьшение возможности совершения сотрудниками ошибок и нарушений в рамках предоставленных им прав и полномочий.

6.4. Организационные (административные) меры защиты

Организационные (административные) меры защиты - это меры организационного характера, регламентирующие процессы функционирования системы обработки информации, 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 или снизить размер потерь в случае их реализации.

6.5. Формирование политики безопасности

Главная цель административных мер, предпринимаемых на высшем управленческом уровне - сформировать политику в области обеспечения безопасности информации (отражающую подходы к защите информации) и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

С практической точки зрения политику в области обеспечения безопасности информации в **МБДОУ № 6** целесообразно разбить на два уровня. К верхнему уровню относятся решения руководства, затрагивающие деятельность **МБДОУ № 6** в целом. Политика верхнего уровня должна четко очертить сферу влияния и ограничения при определении целей безопасности информации, определить какими ресурсами (материальными, структурными, организационными) они будут достигнуты, и найти разумный компромисс между приемлемым уровнем безопасности и функциональностью.

Политика нижнего уровня, определяет процедуры, и правила достижения целей и решения задач безопасности информации и детализирует (регламентирует) эти правила:

– каковы роли и обязанности должностных лиц, отвечающие за проведение политики безопасности информации;

– кто имеет права доступа к информации, кто и при каких условиях может читать и модифицировать информации и т.д.

Политика нижнего уровня должна:

– предусматривать регламент информационных отношений, исключающих возможность произвольных, монопольных или несанкционированных действий в отношении информационных ресурсов;

– определять коалиционные и иерархические принципы и методы разделения секретов и разграничения доступа к информации;

– выбирать программно-технические (аппаратные) средства противодействия НСД, аутентификации, авторизации, идентификации и других защитных механизмов, обеспечивающих гарантии реализации прав и ответственности субъектов информационных отношений.

6.6. Регламентация доступа в помещения

Компоненты информационных систем должны размещаться в помещениях, находящихся под охраной или наблюдением, исключающим возможность бесконтрольного проникновения в помещения посторонних лиц и обеспечивающим физическую сохранность находящихся в помещении защищаемых ресурсов (документов, АРМ и т.п.). Уборка таких помещений должна производиться в присутствии ответственного сотрудника, за которым закреплены данные компоненты, с соблюдением мер, исключающих доступ посторонних лиц к защищаемым информационным ресурсам.

Все посторонние лица допускаются в помещения с компонентами информационной системы только в присутствии сотрудников Управления.

По окончании рабочего дня, помещения, в которых размещаются компоненты информационных систем **МБДОУ № 6**, должны запираться на ключ, по возможности опечатываться.

В случае оснащения помещений средствами охранной сигнализации, а также автоматизированной системой приема и регистрации сигналов от этих средств, прием-сдача таких помещений под охрану осуществляется на основании специально разрабатываемой инструкции.

6.7. Регламентация допуска сотрудников к использованию информационных ресурсов

В рамках разрешительной системы (матрицы) доступа устанавливается: кто, кому, какую информацию и для какого вида доступа может предоставить и при каких условиях.

Допуск пользователей к работе с информационными системами и доступ к их ресурсам должен быть строго регламентирован. Любые изменения состава и полномочий пользователей подсистем должны производиться установленным порядком.

Уровень полномочий каждого пользователя определяется индивидуально, соблюдая следующие требования:

– каждый сотрудник пользуется только предписанными ему правами по отношению к информации, с которыми ему необходима работа в соответствии с должностными обязанностями. Расширение прав доступа и предоставление доступа к дополнительным информационных ресурсам, в обязательном порядке, должно согласовываться с администратором безопасности информации;

– руководитель **МБДОУ № 6** имеет права на просмотр информации своих подчиненных только в установленных пределах в соответствии со своими должностными обязанностями.

Все сотрудники **МБДОУ № 6** и обслуживающий персонал, должны нести персональную ответственность за нарушения установленного порядка обработки информации, правил хранения, использования и передачи находящихся в их распоряжении защищаемых ресурсов системы. Каждый сотрудник (при приеме на работу) должен подписывать обязательство о соблюдении и ответственности за нарушение установленных требований по сохранению информации **МБДОУ № 6**

Обработка ПДн в компонентах информационных систем МБДОУ № 6 должна производиться в соответствии с утвержденными технологическими инструкциями.

6.8. Регламентация процессов обслуживания и осуществления модификации аппаратных и программных ресурсов

В целях поддержания режима информационной безопасности аппаратно-программная конфигурация автоматизированных рабочих мест сотрудников Управления, с которых возможен доступ к ресурсам информационной системы, должна соответствовать кругу возложенных на данных пользователей функциональных обязанностей.

В компонентах информационной системы и на рабочих местах пользователей должны устанавливаться и использоваться лицензионные программные средства.

6.9. Обеспечение и контроль физической целостности (неизменности конфигурации) аппаратных ресурсов

Оборудование информационных систем, используемое для доступа и хранения информации, к которому доступ обслуживающего персонала в процессе эксплуатации не требуется, после наладочных, ремонтных и иных работ, связанных с доступом к его компонентам должно закрываться.

6.10. Подбор и подготовка персонала, обучение пользователей

Пользователи информационных систем **МБДОУ № 6**, а также руководящий и обслуживающий персонал должны быть ознакомлены со своим уровнем полномочий, а также организационно-распорядительной, нормативной, технической и эксплуатационной документацией, определяющей требования и порядок обработки информации в **МБДОУ № 6**.

Обеспечение безопасности информации возможно только после выработки у пользователей определенной культуры работы, т.е. норм, обязательных для исполнения всеми, кто работает с информационными ресурсами Управления. К таким нормам можно отнести запрещение любых умышленных или неумышленных действий, которые нарушают нормальную работу компонентов информационных систем, вызывают дополнительные затраты ресурсов, нарушают целостность хранимой и обрабатываемой информации, нарушают интересы законных пользователей, владельцев или собственников.

Все пользователи информационных систем должны быть ознакомлены с организационно - распорядительными документами по обеспечению безопасности информации (ПДн) **МБДОУ № 6**, в части, их касающейся, должны знать и неукоснительно выполнять инструкции и знать общие обязанности по обеспечению безопасности информации. Доведение требований указанных документов до лиц, допущенных к обработке защищаемой информации, должно осуществляться под роспись.

6.11. Ответственность за нарушения установленного порядка пользования ресурсами информационной системы

Мера ответственности персонала за действия, совершенные в нарушение установленных правил обеспечения безопасной работы с информацией, должна определяться нанесенным ущербом, наличием злого умысла и другими факторами по усмотрению руководства **МБДОУ № 6**.

Для реализации принципа персональной ответственности пользователей за свои действия необходимы:

– индивидуальная идентификация пользователей и инициированных ими процессов, т.е. установление за ними идентификатора (login, Username), на базе которого будет осуществляться разграничение доступа в соответствии с принципом обоснованности доступа;

– проверка подлинности пользователей (аутентификация) на основе паролей;

– реакция на попытки несанкционированного доступа (сигнализация, блокировка и т.д.).

6.12. Средства обеспечения безопасности информации

Для обеспечения информационной безопасности используются следующие средства защиты:

Физические средства защиты

Физические меры защиты основаны на применении разного рода механических, электронных или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также технических средств визуального наблюдения, связи и охранной сигнализации.

Для обеспечения физической безопасности компонентов информационных систем необходимо осуществлять ряд организационных и технических мероприятий, включающих: проверку оборудования, предназначенного для обработки информации, на:

– наличие специально внедренных закладных устройств;

– введение дополнительных ограничений по доступу в помещения, предназначенные для хранения и обработки информации;

– оборудование систем информатизации устройствами защиты от сбоев электропитания и помех в линиях связи.

Технические средства защиты

Технические (аппаратно-программные) меры защиты основаны на использовании различных электронных устройств и специальных программ и

выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.).

С учетом всех требований и принципов обеспечения безопасности информации по всем направлениям защиты в состав системы защиты должны быть включены следующие средства:

– средства разграничения доступа к данным;

– средства регистрации доступа к компонентам информационной системы и контроля за использованием информации;

– средства реагирования на нарушения режима информационной безопасности.

На технические средства защиты возлагается решение следующих основных задач:

– идентификация и аутентификация пользователей при помощи имен или специальных аппаратных средств;

– регламентация и управление доступом пользователей в помещения, к физическим и логическим устройствам;

– защита от проникновения компьютерных вирусов и разрушительного воздействия вредоносных программ;

– регистрация всех действий пользователя в защищенном журнале, наличие нескольких уровней регистрации;

– защита данных системы защиты на файловом сервере от доступа пользователей, в чьи должностные обязанности не входит работа с информации, находящейся на нем.

Средства идентификации и аутентификации пользователей

В целях предотвращения работы с ресурсами информационных систем посторонних лиц необходимо обеспечить возможность распознавания каждого легального пользователя (или групп пользователей). Для идентификации могут применяться различного рода устройства: магнитные карточки, ключи, ключевые вставки, дискеты и т.п.

Аутентификация (подтверждение подлинности) пользователей также может осуществляться:

– путем проверки наличия у пользователей каких-либо специальных устройств (магнитных карточек, ключей, ключевых вставок и т.д.);

– путем проверки знания ими паролей;

– путем проверки уникальных физических характеристик и параметров самих пользователей при помощи специальных биометрических устройств.

Средства разграничения доступа

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

Технические средства разграничения доступа должны по возможности быть составной частью единой системы контроля доступа:

– на контролируемую территорию;

– в отдельные помещения;

– к компонентам информационной среды и элементам системы защиты ПДн (физический доступ);

– к информационным ресурсам (документам, носителям информации, файлам, наборам данных, архивам, справкам и т.д.);

– к активным ресурсам (прикладным программам, задачам и т.п.);

– к операционной системе, системным программам и программам защиты.

Средства обеспечения и контроля целостности

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

Средства контроля целостности информационных ресурсов систем предназначены для своевременного обнаружения модификации или искажения ресурсов системы. Они позволяют обеспечить правильность функционирования системы защиты и целостность хранимой и обрабатываемой информации.

Контроль целостности информации и средств защиты, с целью обеспечения неизменности информационной среды, определяемой предусмотренной технологией обработки, и защиты от несанкционированной модификации информации должен обеспечиваться:

– средствами разграничения доступа (в помещения, к документам, к носителям информации, к серверам, логическим устройствам и т.п.);

– средствами электронной подписи;

– средствами подсчета контрольных сумм (для используемого программного обеспечения).

Средства оперативного контроля и регистрации событий безопасности

Средства объективного контроля должны обеспечивать обнаружение и регистрацию всех событий (действий пользователей, попыток НСД и т.п.), которые могут повлечь за собой нарушение безопасности и привести к возникновению кризисных ситуаций. Анализ собранной средствами регистрации информации позволяет выявить факты совершения нарушений, их характер, подсказать метод его расследования и способы поиска нарушителя и исправления ситуации. Средства контроля и регистрации должны предоставлять возможности:

– ведения и анализа журналов регистрации событий безопасности (системных журналов);

– получения твердой копии (печати) журнала регистрации событий безопасности;

– упорядочения журналов, а также установления ограничений на срок их хранения;

– оперативного оповещения администратора безопасности информации о нарушениях.

При регистрации событий безопасности в журнале должна фиксироваться следующая информация:

– дата и время события;

– идентификатор субъекта, осуществляющего регистрируемое действие;

– действие (тип доступа).

6.13. Контроль эффективности системы защиты

Контроль эффективности защиты информации осуществляется с целью своевременного выявления и предотвращения утечки информации за счет несанкционированного доступа, а также предупреждения возможных специальных воздействий, направленных на уничтожение информации, разрушение средств информатизации. Контроль может проводиться привлекаемыми для этой цели организациями, имеющими лицензию на этот вид деятельности.

Оценка эффективности мер защиты информации проводится с использованием технических и программных средств контроля на предмет соответствия установленным требованиям.