Приложение
к приказу исполняющего обязанности директора
департамента по информационным технологиям
от «08» августа 2017 № 685

Исполняющий обязанности директора
департамента по информационным технологиям

_____ М.В. Егоров

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПАО «ДЕТСКИЙ МИР» ПТ-ДИТ-033-02

СОДЕРЖАНИЕ

ОБЩИЕ ПОЛОЖЕНИЯ 3

1.1. Назначение 3

1.2. Регламентирующие документы 4

1.3. Вводимые определения терминов, сокращений и ролей 4

2. ОБЪЕКТЫ ЗАЩИТЫ 5

3. ЦЕЛИ И ЗАДАЧИ 5

4. ОСНОВНЫЕ ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 5

5. ОСНОВНЫЕ УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В АС 7

5.1. Угрозы безопасности информации и их источники. 7
5.1.1. Основные угрозы безопасности информации 7
5.1.2. Основные источники угроз безопасности информации 8

5.2. Пути реализации искусственных угроз безопасности информации в АС 8

5.3. Умышленные действия сторонних лиц, пользователей и обслуживающего персонала 9

5.4. Неформальная модель возможных нарушителей 10

6. МЕРЫ, МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ТРЕБУЕМОГО УРОВНЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ РЕСУРСОВ 10

6.1. Правовые меры. 10

6.2. Морально-этические меры. 11

6.3. Организационные (административные) меры 11

6.4. Физические меры. 11

6.5. Технические (аппаратно-программные) и технологические меры. 12

7. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ 13

ОБЩИЕ ПОЛОЖЕНИЯ

Тип документа:	Политика		
Аннотация:	Определяет совокупность правил, требований и подходы в области информационной безопасности, которыми руководствуется ПАО «Детский Мир»		
Максимальная периодичность пересмотра:	По мере необходимости	**Минимальная периодичность пересмотра:**	По мере необходимости
Ограничения доступа:	Без ограничений.		

1.1. Назначение

Настоящая Политика информационной безопасности (далее по тексту – Политика) излагает систему взглядов, цели, задачи и определяет совокупность правил, требований и подходы в области информационной безопасности, которыми руководствуется ПАО «Детский Мир» (далее по тексту – Компания).

Политика является основополагающим документом по обеспечению информационной безопасности Компании.

Основные положения и требования Политики распространяются на все структурные подразделения Компании, в которых осуществляется обработка информации, содержащей сведения, подлежащие защите в соответствии с действующим законодательством Российской Федерации и нормативными документами Компании, а также на подразделения, осуществляющие сопровождение, обслуживание и обеспечение штатного (бесперебойного) функционирования автоматизированных систем (далее по тексту – АС). Основные положения Политики могут быть распространены также на подразделения других организаций и учреждений, осуществляющие взаимодействие с АС Компании в качестве поставщиков и потребителей (пользователей) информации, содержащейся в АС.

Политика является методологической основой для:

- Формирования, внедрения и повседневного использования единой политики в области обеспечения информационной безопасности;
- принятия управленческих решений, разработки практических мер по реализации единой политики информационной безопасности Компании, выработки комплекса, согласованных мер нормативно-правового, технологического и организационно-технического характера, направленных на выявление, отражение, локализацию и ликвидацию последствий реализации различных видов угроз безопасности информации;
- координации деятельности структурных подразделений ПАО «Детский Мир» при проведении работ по созданию, развитию и эксплуатации АС с соблюдением требований информационной безопасности;
- разработки предложений по совершенствованию правового, нормативного, методического, технического и организационного обеспечения информационной безопасности.

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, а также текущее состояние и перспективы развития информационных технологий.

Политика пересматривается не реже 1 раза в 5 лет.

1.2. Регламентирующие документы

Политика основывается на требованиях действующего законодательства Российской Федерации и нормативных актов органов государственной власти Российской Федерации.

1.3. Вводимые определения терминов, сокращений и ролей

Таблица 1. Перечень сокращений

Сокращение	Расшифровка сокращения
НСД	Несанкционированный доступ
ЛВС	Локально-вычислительная сеть
ПО	Программное обеспечение
ДИТ	Департамент по информационным технологиям
ДКБ	Департамент корпоративной безопасности
ИБ	Информационная безопасность
ТКС	Телекоммуникационная сеть
СЗИ	Система(средства) защиты информации
АС	Автоматизированная система

Таблица 2. Перечень терминов

Наименование термина	Определение термина
Компания	ПАО «Детский мир»
Коммерческая тайна	Режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду;
Информация, составляющая КТ	Сведения любого характера (производственные, технические, экономические, организационные и другие), а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых Компанией введен режим коммерческой тайны;
Мультивендорный подход	Использование услуг/оборудования нескольких производителей как средство дополнительных мер обеспечения безопасности информационных объектов

Таблица 3. Область применения

Наименование должности/роли	ЦО	РО	Магазины
Все сотрудники, а также лица, состоящие в договорных отношениях с ПАО «Детский мир»;	X	X	X

2. Объекты защиты

Основными объектами информационной безопасности в ПАО «Детский Мир» являются:

- информационные ресурсы с ограниченным доступом, подлежащие защите в соответствии с действующим законодательством Российской Федерации и нормативными документами ПАО «Детский Мир», 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 данных, независимо от формы и вида их представления;

- 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 компоненты АС.

3. Цели и задачи

Обеспечение информационной безопасности является неотъемлемой частью работы ПАО «Детский Мир». Под обеспечением информационной безопасности понимается комплекс организационных и технологических мер/мероприятий (в дальнейшем по тексту – Комплекс мероприятий), которые включают: подходы, порядки, процедуры, технические и технологические решения, а также другие меры/мероприятия, направленные на защиту информации.

Под защитой информации понимается обеспечение её конфиденциальности, доступности, достоверности и целостности.

Основной целью Комплекса мероприятий по обеспечению информационной безопасности является создание условий устойчивого функционирования Компании путем предотвращения угроз, действующих в отношении хранимой и обрабатываемой в АС Компании информации, а также как на снижение вероятности реализации самих угроз, так и на минимизацию возможного ущерба от их реализации.

Задачами Комплекса мероприятий по обеспечению безопасности информации являются:

- Обеспечение защиты информации, хранимой и обрабатываемой в АС Компании.
- Снижение вероятности возникновения угроз, действующих в отношении информации, и минимизация негативных последствий при реализации этих угроз.
- Обеспечение минимального, приемлемого для подразделений Компании, времени восстановления АС при реализации угроз информационной безопасности.
- Восстановление функционирования АС в штатном режиме.

4. Основные принципы обеспечения информационной безопасности

Общая цель подразделений Департамента информационных технологий и подразделений Департамента корпоративной безопасности ПАО «Детский Мир» – предоставление надежных, эффективных и экономически целесообразных решений для

сотрудников Компании и увеличения эффективности их работы, доступа к внешним источникам информации, удобства для конечных пользователей, обеспечение быстрого взаимодействия с бизнес партнерами, в то же время обеспечивая конфиденциальность, целостность и доступность информации в информационных системах.

Обеспечение информационной безопасности ПАО «Детский Мир» строится на следующих принципах:

- Комплексность

  Под комплексностью понимается обеспечение безопасности информационных ресурсов в течение всего их жизненного цикла, на всех технологических этапах обработки (преобразования) и использования информации, во всех режимах функционирования информационных ресурсов всеми доступными законными средствами, методами и мероприятиями, а также способность системы к развитию и совершенствованию в соответствии с изменениями условий функционирования. Комплексность достигается совокупностью правовых, организационных и инженерно-технических мероприятий.

  Технические, технологические и организационные решения, обеспечивающие безопасность информации, должны прорабатываться при внедрении новых и/или изменении уже существующих бизнес-процессов, разработке новых (проектируемых) и/или изменении функционирующих АС.
- Целостность и непротиворечивость

  Комплекс мероприятий по обеспечению информационной безопасности разрабатывается и применяется как целостная система для всей сети Компании. Мероприятия, разработанные для отдельных бизнес-процессов, группы бизнес-процессов, АС и подразделений не должны противоречить друг другу и строятся на единых подходах и принципах.
- Своевременность

  Под своевременностью понимается упреждающий характер мер/мероприятий по обеспечению информационной безопасности, основанный на прогнозировании возникновения угроз в отношении безопасности информации, АС и информационных систем, анализе рисков и предполагаемых потерь.
- Непрерывность и актуальность

  Означает непрерывность и действенность (актуальность) принимаемых мер/мероприятий по обеспечению безопасности информации. Комплекс мероприятий по обеспечению информационной безопасности действует постоянно. Кроме того, для обеспечения актуальности применяемых мер/мероприятий на периодической основе, должен проводиться их аудит на предмет соответствия применяемых мер/мероприятий и их способности противостоять новым угрозам информационной безопасности.
- Преемственность и совершенствование

  Предполагает постоянное совершенствование мер и средств защиты информации на основе преемственности организационных, технологических и технических решений, анализа функционирования АС и их систем/средств защиты с учетом изменений в методах и средствах перехвата информации, появлении новых угроз безопасности информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.
- Экономическая целесообразность

  Экономическая целесообразность – сопоставимость возможного ущерба и затрат на обеспечение информационной безопасности. Во всех случаях стоимость решений по обеспечению информационной безопасности не должна быть больше стоимости возможного ущерба от любых видов рисков или их совокупности за определенный период времени.
- Взаимодействие и координация

Означает осуществление мер/мероприятий по обеспечению информационной безопасности на основе:

- взаимодействия между соответствующими подразделениями и службами ПАО «Детский Мир»;
- взаимодействия между подразделениями Компании и сторонними организациями, специализирующимися на разработке и/или внедрении в ПАО «Детский Мир» бизнес-технологий, технических, технологических решений, поставке услуг и т.д.;
- четкого разделения полномочий и ответственности между подразделениями компании;
- координации действий подразделений по обеспечению информационной безопасности.

- Централизация управления

  Предполагает функционирование Комплекса мероприятий по обеспечению информационной безопасности по единым правовым, организационным, функциональным и методологическим принципам и централизованное управление ее деятельностью.
- Персональная ответственность

  Означает ответственность руководителей подразделений компании и их сотрудников за соблюдение требований нормативных и нормативных документов ПАО «Детский Мир» по информационной безопасности. Руководители подразделений Компании несут персональную ответственность за ознакомление сотрудников их подразделений с документами по информационной безопасности.
- Принцип минимизации полномочий

  Соблюдение принципа минимальной достаточности - означает предоставление пользователям минимально необходимых для выполнения его должностных обязанностей прав доступа к АС.
- Законность

  Означает соответствие организационных, технических и технологических решений требованиям федерального законодательства Российской Федерации, нормативных актов органов государственной власти, нормативных документов ПАО «Детский Мир» с применением всех дозволенных методов обнаружения и пресечения правонарушений при работе с информацией.

  Принятые меры безопасности информации не должны препятствовать доступу правоохранительных органов в предусмотренных действующим законодательством случаях к информации конкретных систем.

5. Основные угрозы безопасности информации, обрабатываемой АС ПАО «Детский Мир»

5.1. Угрозы безопасности информации и их источники.

5.1.1. Основные угрозы безопасности информации

Основными угрозами безопасности информации, хранимой и обрабатываемой в АС Компании (способами нанесения ущерба субъектам информационных отношений) являются:

- нарушение конфиденциальности (разглашение, утечка) сведений, составляющих коммерческую тайну ПАО «Детский Мир», а также иную информацию, защищаемую компанией в соответствии с законодательством Российской Федерации;
- нарушение работоспособности (дезорганизация работы) АС Компании, блокирование информации, нарушение технологических процессов, срыв своевременного решения задач, нарушение доступности самих АС и приложений;
- нарушение целостности (искажение, подмена, уничтожение) информационных, программных и других ресурсов АС Компании, а также фальсификация (подделка) документов.

5.1.2. Основные источники угроз безопасности информации

Основными источниками угроз безопасности информации АС, приводящие к непроизводительным затратам времени и ресурсов, разглашению сведений ограниченного распространения, потере ценной информации или нарушению работоспособности отдельных рабочих станций, подсистем или АС в целом, являются:

- непреднамеренные (ошибочные, случайные, необдуманные, без злого умысла и корыстных побуждений) нарушения установленных регламентов сбора, обработки и передачи информации, а также требований безопасности информации и другие действия сотрудников (в том числе администраторов АС) структурных подразделений Компании при эксплуатации соответствующих АС;
- преднамеренные (из корыстных побуждений, по принуждению третьими лицами, со злым умыслом и т.п.) действия сотрудников Компании, допущенных к работе с соответствующими АС, а также сотрудников подразделений, отвечающих за обслуживание, администрирование программного и аппаратного обеспечения, средств защиты и обеспечения безопасности информации;
- воздействия из других логических и физических сегментов АС со стороны сотрудников других подразделений, в том числе разработчиков, а также удаленное несанкционированное вмешательство посторонних лиц, как из телекоммуникационной сети (ТКС) Компании, так и внешних сетей общего назначения (через легальные и несанкционированные каналы подключения компании к таким сетям), в том числе, используя недостатки протоколов обмена, средств защиты и разграничения удаленного доступа к ресурсам АС;
- деятельность криминальных групп, политических и экономических структур, а также отдельных лиц по добыванию информации, навязыванию ложной информации, нарушению работоспособности системы в целом и ее отдельных компонент;
- ошибки, допущенные при проектировании АС и ее системы защиты, ошибки в программном обеспечении, отказы и сбои технических средств (в том числе средств защиты информации и их контроля) АС;
- аварии, стихийные бедствия.

5.2. Пути реализации искусственных угроз безопасности информации в АС ПАО «Детский Мир»

Пользователи, операторы, системные администраторы и сотрудники ПАО «Детский Мир», обслуживающие систему, являются внутренними источниками случайных воздействий, так как имеют непосредственный доступ к процессам обработки информации и могут совершать непреднамеренные ошибки и нарушения действующих правил, инструкций и процедур.

Основные пути реализации непреднамеренных искусственных угроз АС (действия, совершаемые людьми случайно, по незнанию, невнимательности или халатности, из любопытства, но без злого умысла):

- действия сотрудников Компании, приводящие к частичному или полному отказу работоспособности АС в целом либо их компонентов (подсистем) или нарушению работоспособности аппаратных или программных средств; отключению оборудования или изменение режимов работы устройств и программ; разрушению информационных ресурсов АС или их подсистем (неумышленная порча оборудования, удаление, искажение программ или файлов с важной информацией, в том числе системных, повреждение каналов связи, неумышленная порча носителей информации и т.п.);
- несанкционированный запуск технологических программ и процессов, способных при некомпетентном использовании вызывать потерю работоспособности АС или их подсистем

(зависания или зацикливания) или осуществляющих необратимые изменения в них (форматирование или реструктуризацию носителей информации, удаление данных и т.п.);
- несанкционированное внедрение и использование неучтенных программ (игровых, обучающих, технологических и других, не являющихся необходимыми для выполнения сотрудниками своих служебных обязанностей) с последующим необоснованным расходованием ресурсов (процессорного времени, оперативной памяти, памяти на внешних носителях и т.п.);
- непреднамеренное заражение компьютера вирусами;
- разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования или электронно-цифровых подписей, идентификационных карточек, пропусков и т.п.);
- игнорирование организационных ограничений (установленных правил) при работе в АС ПАО «Детский Мир»;
- некомпетентное использование, настройка или неправомерное отключение средств защиты администраторами, пользователями или персоналом подразделения безопасности;
- ввод ошибочных данных.

Меры по минимизации угроз и снижению возможного ущерба от их реализации определяются в каждом конкретном случае, как при разработке новых бизнес-процессов или внесении изменений в существующие, так и реализации технических и технологических проектов по автоматизации соответствующих бизнес-процессов.

5.3. Умышленные действия сторонних лиц, пользователей и обслуживающего персонала

Основные возможные пути умышленной дезорганизации работы, вывода АС или их компонентов из строя, проникновения в АС ПАО «Детский Мир» и несанкционированного доступа к информации (с корыстными целями, по принуждению, из желания отомстить и т.п.):
- физическое разрушение или вывод из строя всех или отдельных наиболее важных компонентов АС (устройств, носителей важной системной информации, лиц из числа персонала и т.п.), отключение или вывод из строя подсистем обеспечения функционирования АС и/или их компонент (электропитания, линий связи, вентиляции и т.п.);
- внедрение агентов в число персонала ПАО «Детский Мир» (в том числе, и в подразделения Компании, отвечающие за администрирование и безопасность), вербовка (путем подкупа, шантажа, угроз и т.п.) пользователей, имеющих определенные полномочия по доступу к защищаемым ресурсам;
- хищение носителей информации (распечаток, магнитных дисков, лент, микросхем памяти, запоминающих устройств и целых ЭВМ), хищение производственных отходов (распечаток, записей, списанных носителей информации и т.п.);
- несанкционированное копирование носителей информации, чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
- несанкционированная модификация программного обеспечения – внедрение программных "закладок" и "вирусов" ("троянских коней" и "жучков"), то есть участков программ (программного кода), которые не нужны для осуществления заявленных функций, но позволяющих преодолевать систему защиты, скрытно и незаконно осуществлять доступ к системным ресурсам с целью регистрации и передачи защищаемой информации или дезорганизации функционирования системы;

- перехват данных, передаваемых по каналам связи, и их анализ с целью получения конфиденциальной информации и выяснения протоколов обмена, правил установления соединений и авторизации пользователей и последующих попыток их имитации для проникновения в систему;
- вмешательство в процесс функционирования АС из сетей общего пользования с целью несанкционированного доступа к защищаемой информации, модификации данных, дезорганизации работы АС и их компонент и т.п.

5.4. Неформальная модель возможных нарушителей

Нарушитель – это лицо, которое предприняло попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или удовольствия, с целью самоутверждения и т.п.) и использующее для этого различные возможности, методы и средства.

Комплекс мероприятий по обеспечению информационной безопасности ПАО «Детский Мир» основывается на том, что система защиты должна успешно противостоять и/или регистрировать несанкционированные действия сотрудников, зарегистрированных как пользователь АС, действующий целенаправленно из корыстных интересов, возможно в сговоре с лицами, не являющимися сотрудниками компании.

При этом нарушитель может использовать весь набор методов и средств взлома как самих АС и их компонент, так и систем защиты, включая агентурные методы получения реквизитов доступа, методы социальной инженерии, пассивные средства (технические средства перехвата информации), методы и средства активного воздействия (модификация технических средств, подключение к каналам передачи данных, внедрение программных закладок и использование специальных инструментальных и технологических программ), а также комбинации воздействий как из внутренней ЛВС Компании, так и со стороны внешних сетей – из сетей общего пользования, например сети Интернет.

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

Комплекс мероприятий по обеспечению информационной безопасности состоит из следующих мер:

- правовые (законодательные);
- морально-этические;
- организационные (административные);
- физические;
- технические и технологические (аппаратные и программные).

6.1. Правовые меры.

К правовым мерам защиты относится федеральное законодательство Российской Федерации, нормативные документы органов государственной власти Российской Федерации и нормативные документы ПАО «Детский Мир», регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих законодательных и нормативных актов, препятствуя тем самым неправомерному использованию информации и являющиеся сдерживающим фактором для потенциальных нарушителей.

Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной (профилактической) работы с пользователями и обслуживающим персоналом.

Пользователи и обслуживающий персонал АС должны иметь представление об ответственности за правонарушения в области информационной безопасности. Любые нарушения порядка и правил работы в АС сотрудниками структурных подразделений должны расследоваться. К виновным должны применяться соответствующие меры воздействия. Мера ответственности персонала за действия, совершенные в нарушение установленных правил обеспечения безопасной автоматизированной обработки информации, должна определяться с учетом нанесенного ущерба, наличием злого умысла и другими факторами по усмотрению Генерального директора Компании.

6.2. Морально-этические меры.

К морально-этическим мерам относятся нормы поведения, большей частью не являющиеся обязательными, как правовые меры защиты, однако, их несоблюдение может вести к падению авторитета, престижа человека, группы лиц или организации.

Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в коллективах подразделений.

6.3. Организационные (административные) меры.

Организационные (административные) меры защиты являются мерами организационного характера, регламентирующими процессы функционирования АС ПАО «Детский Мир» и их компонент, использование ресурсов АС, действия обслуживающего персонала по поддержанию функционирования АС в штатном режиме и т.д.

Кроме того, организационные меры регламентируют порядок взаимодействия пользователей АС, направленный на затруднение или исключение возможности реализации угроз безопасности, снижение вероятности их реализации и/или снижение потерь, в том числе финансовых, в случае их реализации.

Главная цель административных мер, предпринимаемых Руководством ПАО «Детский Мир» – сформировать политику в области обеспечения безопасности информации (отражающую подходы к защите информации) и обеспечить ее выполнение, выделяя необходимые ресурсы и осуществляя контроль над общим уровнем защищенности информации.

6.4. Физические меры.

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

Физическая защита зданий, помещений, объектов и средств информатизации осуществляется, с помощью технических средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими проникновение в здание, помещения посторонних лиц, хищение документов и информационных носителей, самих

средств информатизации, исключающими нахождение внутри контролируемой (охраняемой) зоны технических средств разведки.

6.5. Технические (аппаратно-программные) и технологические меры.

Технические (аппаратно-программные) меры защиты основываются на использовании различных средств защиты информации от несанкционированного доступа к защищаемой Компанией информации, как на уровне приложений, так и на уровне обеспечения защиты каналов связи. Указанные средства могут входить в состав системы Компании или использоваться в автономном режиме, если это определено бизнес-процессом.

Средства защиты должны обеспечивать многоуровневую схему обеспечения безопасности (эшелонированная система безопасности) и выбираются исходя из «мультивендорного подхода». С учетом всех требований и принципов обеспечения безопасности информации в АС по всем направлениям защиты в состав системы защиты должны быть включены следующие средства:

- средства аутентификации потребителей (пользователей) и компонентов АС ПАО «Детский Мир» (терминалов, задач, элементов баз данных и т.п.), соответствующих степени конфиденциальности информации и обрабатываемых данных;
- средства разграничения доступа к данным, самим АС и их компонентам;
- средства криптографического закрытия информации в каналах связи и в базах данных;
- средства регистрации доступа и контроля за использованием защищаемой информации;
- средства обнаружения и реагирования на попытки получения несанкционированного доступа (как успешные, так и неуспешные);

Технологические меры защиты основываются на использовании различных технологических решений и систем, обеспечивающих защиту информации от несанкционированного доступа.

На технические и технологические средства защиты от несанкционированного доступа к защищаемой Компанией информации возлагается решение следующих основных задач:

- идентификация и аутентификации пользователей по уникальным идентификаторам и/или специальным аппаратным средствам;
- регламентация предоставления и аннулирования доступа пользователей;
- создание замкнутой программной среды разрешенных для запуска программ;
- защита от проникновения компьютерных вирусов и разрушительного воздействия вредоносных программ;
- контроль целостности модулей системы защиты;
- регистрация действий пользователя, наличие нескольких уровней регистрации;
- централизованное управление настройками средств разграничения доступа в АС;
- оповещение подразделения информационной безопасности обо всех событиях несанкционированного доступа, происходящего на любом узле АС Компании;
- оперативный контроль за работой пользователей сети, изменение режимов функционирования рабочих станций и возможность блокирования (при необходимости) любой станции сети.

Успешное применение технических и технологических средств защиты предполагает, что выполнение перечисленных ниже требований обеспечено правовыми,

организационными и физическими мерами обеспечения требуемого уровня защищенности информационных ресурсов:

- обеспечена физическая целостность и безопасность всех компонентов АС;
- создана уникальная система идентификации компонентов АС (рабочие станции сотрудников, сервера, сете образующее оборудование и т.д.);
- создана функционально замкнутая аппаратно-программная среда;

7. Заключительные положения

Политика ИБ является основополагающим документом в построении нормативно-распорядительной базы документального обеспечения информационной безопасности ПАО «Детский Мир» и является документом верхнего уровня. Положения документов нижестоящего уровня не могут противоречить друг другу и основным принципам, целям и задачам, изложенным в Политике.

Положения нижестоящих документов исходят из того, что АС ПАО «Детский Мир» являются географически распределенной системой, объединяющей АС и их компоненты всех подразделений в единую корпоративную вычислительную (информационно-телекоммуникационную) сеть.

В АС циркулирует информация разных категорий. Защищаемая информация может быть совместно использована различными пользователями из различных подсетей единой вычислительной сети.

Комплекс технических средств систем ПАО «Детский Мир» включает средства обработки данных (рабочие станции сотрудников, сервера БД, почтовые сервера и т.п.), средства обмена данными в ЛВС с возможностью подключения к глобальным сетям (кабельная система, мосты, шлюзы, модемы и т.д.), а также средства резервного копирования и восстановления (в том числе, хранения) данных.

К основным особенностям функционирования АС относятся:

- территориальная «распределённость» системы;
- объединение в единую систему большого количества разнообразных технических средств обработки и передачи информации;
- разнообразие решаемых задач и типов обрабатываемых сведений (данных), сложные режимы автоматизированной обработки информации, совмещенные с информационными запросами различных пользователей;
- объединение в базах данных информации различного назначения, принадлежности и уровней конфиденциальности;
- непосредственный доступ к вычислительным и информационным ресурсам различных категорий пользователей (источников и потребителей информации) и обслуживающего персонала;
- наличие каналов взаимодействия с "внешним миром" (источниками и потребителями информации);
- требования по обеспечению непрерывности функционирования бизнес-процессов, и АС ПАО «Детский Мир»;
- высокая интенсивность информационных потоков в ЛВС и АС;
- наличие в АС ярко выраженных функциональных подсистем с различными требованиями по уровням защищенности (физически объединенных в единую сеть);

- разнообразие категорий пользователей и обслуживающего персонала АС.

Единая телекоммуникационная информационная система представляет собой совокупность ЛВС объектов ПАО «Детский Мир», объединенных средствами телекоммуникации. Каждая ЛВС объединяет ряд взаимосвязанных и взаимодействующих автоматизированных подсистем (технологических участков), обеспечивающих решение задач как отдельными структурными подразделениями.

8. Контроль версий документа

Номер версии	Дата создания версии	Должность Ответственного за разработку	ФИО Ответственного за разработку	Краткое описание изменений документа
1	17.08.2015	Специалист сектора ИБ	Фисенко К.И.	Создание документа
2	15.02.2017	Менеджер по системам безопасности и видео наблюдению	Киселёв К.В.	Актуализация