Введено в действие
приказом директора школы
№213 от 29 августа 2019г.

Принято
на педагогическом совете школы
Протокол №1 от 29 августа 2019г.

Утверждаю
Директор МБОУ «СОШ №32 с углубленным изучением отдельных предметов»
_____ В.И. Рагузина

Положение
об информационной безопасности

Муниципального бюджетного образовательного учреждения
«Средняя общеобразовательная школа №32
с углубленным изучением отдельных предметов»

Политика информационной безопасности Муниципального бюджетного образовательного учреждения «Средняя общеобразовательная школа №32 с углубленным изучением отдельных предметов»

1. Общие положения

1.1. Политика информационной безопасности (далее – Политика ИБ) Муниципального бюджетного образовательного учреждения «Средняя общеобразовательная школа №32 с углубленным изучением отдельных предметов» (далее – МБОУ «СОШ №32 с углубленным изучением отдельных предметов») определяет цели и задачи системы обеспечения информационной безопасности и устанавливает совокупность правил, требований и руководящих принципов в области информационной безопасности, которыми руководствуется МБОУ «СОШ №32 с углубленным изучением отдельных предметов» в своей деятельности.

1.2. Политика ИБ учитывает современное состояние и ближайшие перспективы развития информационных технологий в МБОУ «СОШ №32 с углубленным изучением отдельных предметов», цели, задачи и правовые основы их эксплуатации, режимы функционирования, а также содержит анализ угроз безопасности для объектов и субъектов информационных отношений МБОУ «СОШ №32 с углубленным изучением отдельных предметов».

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

1.4. Информационная безопасность МБОУ «СОШ №32 с углубленным изучением отдельных предметов», заключается в неукоснительном соблюдении всеми сотрудниками

МБОУ «СОШ №32 с углубленным изучением отдельных предметов» требований и принципов, изложенных в Политике ИБ.

1.5. Разработка Политики ИБ, внесение изменений и общий контроль выполнения требований по обеспечению информационной безопасности МБОУ «СОШ №32 с углубленным изучением отдельных предметов» осуществляется Бариновым Е.Г.

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

1.7. Все сотрудники МБОУ «СОШ №32 с углубленным изучением отдельных предметов» 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 МБОУ «СОШ №32 с углубленным изучением отдельных предметов».

1.10. Документами, детализирующими положения Политики ИБ применительно к одной или нескольким областям информационной безопасности, видам и технологиям деятельности МБОУ «СОШ №32 с углубленным изучением отдельных предметов», 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 МБОУ «СОШ №32 с углубленным изучением отдельных предметов» 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 МБОУ «СОШ №32 с углубленным изучением отдельных предметов», независимо от формы и вида ее представления;
- процессы обработки информации в ЕСС МБОУ «СОШ №32 с углубленным изучением отдельных предметов», 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 МБОУ «СОШ №32 с углубленным изучением отдельных предметов», локально-вычислительные сети разного уровня и комплексы автоматизированных

рабочих мест, объединенных в единую структурированную сеть (ЕСС).

2.3. К основным особенностям информационной среды МБОУ «СОШ №32 с углубленным изучением отдельных предметов» относятся:

- объединение в единые системы разнообразных технических и программно-аппаратных средств обработки и передачи информации;
- расширение сферы использования информационных систем МБОУ «СОШ №32 с углубленным изучением отдельных предметов»;
- 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 МБОУ «СОШ №32 с углубленным изучением отдельных предметов»;
- 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 МБОУ «СОШ №32 с углубленным изучением отдельных предметов», независимо от ее представления и местонахождения в ЕСС.

3. Цели и задачи деятельности по обеспечению информационной безопасности

3.1 Основной целью деятельности по обеспечению информационной безопасности МБОУ «СОШ №32 с углубленным изучением отдельных предметов» является защита объектов информационной безопасности МБОУ «СОШ №32 с углубленным изучением отдельных предметов» 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 МБОУ «СОШ №32 с углубленным изучением отдельных предметов»;
- 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 МБОУ «СОШ №32 с углубленным изучением отдельных предметов»;
- Разграничение доступа пользователей к объектам информационной безопасности и иным ресурсам МБОУ «СОШ №32 с углубленным изучением отдельных предметов»;
- Обеспечение аутентификации пользователей, участвующих в информационном обмене;
- Защита от несанкционированной модификации используемых в ЕСС МБОУ «СОШ №32 с углубленным изучением отдельных предметов» 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 МБОУ «СОШ №32 с углубленным изучением отдельных предметов»;
- Регистрацией в журналах действий персонала, осуществляющего обслуживание и модификацию объектов информационной безопасности
- Полнотой, реальной выполнимостью и непротиворечивостью требований организационно – распорядительных документов МБОУ «СОШ №32 с углубленным изучением отдельных предметов» 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 МБОУ «СОШ №32 с углубленным изучением отдельных предметов»;
- Четким знанием и строгим соблюдением всеми пользователями объектов информационной безопасности МБОУ «СОШ №32 с углубленным изучением отдельных предметов», 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 МБОУ «СОШ №32 с углубленным изучением отдельных предметов»;
- Применением физических и технических средств защиты объектов информационной безопасности МБОУ «СОШ №32 с углубленным изучением отдельных предметов» и непрерывной административной поддержкой их использования
- Эффективным контролем над соблюдением пользователями информационных ресурсов МБОУ «СОШ №32 с углубленным изучением отдельных предметов» требований по обеспечению безопасности информации;

4. **Основные угрозы безопасности информации в** МБОУ «СОШ №32 с углубленным изучением отдельных предметов»

4.1 Под угрозами безопасности информации в МБОУ «СОШ №32 с углубленным изучением отдельных предметов» понимается потенциально возможные негативные воздействия на защищаемую информацию.

4.2 Основными источниками угроз безопасности информации в МБОУ «СОШ №32 с углубленным изучением отдельных предметов» 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 МБОУ «СОШ №32 с углубленным изучением отдельных предметов» является источник угрозы;
- Ошибки, допущенные при разработке компонентов объектов информационной безопасности МБОУ «СОШ №32 с углубленным изучением отдельных предметов» и их систем защиты, ошибки в программном обеспечении, отказы и сбои технических средств;
- Аварии, стихийные бедствия.

4.3 Сотрудники МБОУ «СОШ №32 с углубленным изучением отдельных предметов», зарегистрированные как легальные пользователи ЕСС МБОУ «СОШ №32 с углубленным изучением отдельных предметов» 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 МБОУ «СОШ №32 с углубленным изучением отдельных предметов»:

- Неумышленные действия, приводящие к частичному или полному нарушению функциональности компонентов объектов информационной безопасности МБОУ «СОШ №32 с углубленным изучением отдельных предметов» 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 МБОУ «СОШ №32 с углубленным изучением отдельных предметов» 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 МБОУ «СОШ №32 с углубленным изучением отдельных предметов»:

- Умышленные действия, приводящие к частичному или полному нарушению функциональных компонентов объектов информационной безопасности МБОУ «СОШ №32 с углубленным изучением отдельных предметов» или разрушению информационных или программно – технических ресурсов;
- Действия по дезорганизации функционирования объектов информационной безопасности МБОУ «СОШ №32 с углубленным изучением отдельных предметов»; 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 МБОУ «СОШ №32 с углубленным изучением отдельных предметов»;
- Перехват данных, передаваемых по каналам связи и их анализ;
- Хищение производственных отходов;
- Незаконное получение атрибутов разграничения доступа;
- Несанкционированный доступ к объектов информационной безопасности МБОУ «СОШ №32 с углубленным изучением отдельных предметов» 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 МБОУ «СОШ №32 с углубленным изучением отдельных предметов»;
- Незаконное использование оборудования, программных средств или информационных ресурсов.

4.6 Возможные пути реализации основных естественных угроз безопасности МБОУ «СОШ №32 с углубленным изучением отдельных предметов»:

- 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 МБОУ «СОШ №32 с углубленным изучением отдельных предметов» должна строиться исходя из предположений о

возможных типах нарушителей и злоумышленников в системе.

4.10 Некомпетентный пользователь – сотрудник МБОУ «СОШ №32 с углубленным изучением отдельных предметов» использующий только штатные средства, который может предпринимать попытки выполнения запрещенных действий, доступа к защищаемым объектов информационной безопасности МБОУ «СОШ №32 с углубленным изучением отдельных предметов» с превышением своих полномочий, ввода некорректных данных, нарушения правил и регламентов работы с информацией и т.д.

4.11 Любитель – сотрудник МБОУ «СОШ №32 с углубленным изучением отдельных предметов», 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 МБОУ «СОШ №32 с углубленным изучением отдельных предметов», 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 МБОУ «СОШ №32 с углубленным изучением отдельных предметов».

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 МБОУ «СОШ №32 с углубленным изучением отдельных предметов».

4.14 К внутренним нарушителем могут быть отнесены лица из следующих категорий сотрудников МБОУ «СОШ №32 с углубленным изучением отдельных предметов»:

- Зарегистрированные пользователи ЕСС;
- Сотрудники МБОУ «СОШ №32 с углубленным изучением отдельных предметов», не являющиеся зарегистрированными пользователями и не допущенные к ресурсам ЕСКС, но имеющие доступ в здание и помещения;
- Персонал, обеспечивающий обслуживание технические средства объектов информационной безопасности МБОУ «СОШ №32 с углубленным изучением отдельных предметов».
- Специалисты, задействованные в сопровождении программного обеспечения;

4.15 Внешним нарушителем может быть лицо из следующих категорий:

- Уволенные сотрудники МБОУ «СОШ №32 с углубленным изучением отдельных предметов»;
- Представители организаций, взаимодействующих по вопросам технического обеспечения МБОУ «СОШ №32 с углубленным изучением отдельных предметов»;
- Посетители;
- Члены преступных организаций;
- Лица, случайно или умышленно проникшие в ЕСС МБОУ «СОШ №32 с

углубленным изучением отдельных предметов» из внешних телекоммуникационных сетей (хакеры).

5. Основные принципы построения системы информационной безопасности МБОУ «СОШ №32 с углубленным изучением отдельных предметов»

5.1 Законность.

Предполагает осуществление защитных мероприятий и разработку систем безопасности информации МБОУ «СОШ №32 с углубленным изучением отдельных предметов» в соответствии с действующим законодательством в области информационных технологий. Все пользователи объектов информационной безопасности МБОУ «СОШ №32 с углубленным изучением отдельных предметов» должны иметь представление об ответственности за правонарушения в области информационных технологий. Реализация данного принципа необходима для защиты имени и репутации МБОУ «СОШ №32 с углубленным изучением отдельных предметов».

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 МБОУ «СОШ №32 с углубленным изучением отдельных предметов». При создании системы защиты должны учитываться все слабые и наиболее уязвимые места объектов информационной безопасности МБОУ «СОШ №32 с углубленным изучением отдельных предметов». 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 МБОУ «СОШ №32 с углубленным изучением отдельных предметов» и сотрудниками, который должен постоянно идти на всех уровнях внутри МБОУ «СОШ №32 с углубленным изучением отдельных предметов». Каждый сотрудник МБОУ «СОШ №32 с углубленным изучением отдельных предметов» должен приниматься участие в этом процессе. Деятельность по обеспечению информационной безопасности является составной частью повседневной деятельности МБОУ «СОШ №32 с углубленным изучением отдельных предметов».

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 МБОУ «СОШ №32 с углубленным изучением отдельных предметов». МБОУ «СОШ №32 с углубленным изучением отдельных предметов» 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 и оказывать содействие Отделу. Все сотрудники МБОУ «СОШ №32 с углубленным изучением отдельных предметов» 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 МБОУ «СОШ №32 с углубленным изучением отдельных предметов» 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 специалистами МБОУ «СОШ №32 с углубленным изучением отдельных предметов».

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 МБОУ «СОШ №32 с углубленным изучением отдельных предметов» или отдела должны немедленно доводиться до сведения руководителей соответствующего Учреждения 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 МБОУ «СОШ №32 с углубленным изучением отдельных предметов» 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 МБОУ «СОШ №32 с углубленным изучением отдельных предметов» 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 МБОУ «СОШ №32 с углубленным изучением отдельных предметов» разделена на два уровня:

- верхний;
- нижний.

К верхнему уровню политики обеспечения безопасности информации относятся решения руководства, затрагивающие деятельность МБОУ «СОШ №32 с углубленным изучением отдельных предметов» 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

МБОУ «СОШ №32 с углубленным изучением отдельных предметов» 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 МБОУ «СОШ №32 с углубленным изучением отдельных предметов», зарегистрированные как легальные пользователи ЕСС 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 МБОУ «СОШ №32 с углубленным изучением отдельных предметов» 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 МБОУ «СОШ №32 с углубленным изучением отдельных предметов», должно быть запрещено.

6.12 Пользователи объектов информационной безопасности МБОУ «СОШ №32 с углубленным изучением отдельных предметов» должны быть ознакомлены со своим уровнем полномочий, а также организационной – распорядительной, нормативной, технической и эксплуатационной документацией, определяющей требования и порядок обработки информации в МБОУ «СОШ №32 с углубленным изучением отдельных предметов».

6.13 Для непосредственной организации и эффективного функционирования системы обеспечения информационной безопасности, исключающей возможные конфликты интересов, в МБОУ «СОШ №32 с углубленным изучением отдельных предметов» 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 МБОУ «СОШ №32 с углубленным изучением отдельных предметов» 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 МБОУ «СОШ №32 с углубленным изучением отдельных предметов» 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 МБОУ «СОШ №32 с углубленным изучением отдельных предметов» 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 МБОУ «СОШ №32 с углубленным изучением отдельных предметов» 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 МБОУ «СОШ №32 с углубленным изучением отдельных предметов» 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 МБОУ «СОШ №32 с углубленным изучением отдельных предметов» 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 безопасность МБОУ «СОШ №32 с углубленным изучением отдельных предметов», 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 МБОУ «СОШ №32 с углубленным изучением отдельных предметов», ответственного сотрудника.

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.

7.5 Требования Политики ИБ могут развиваться другими внутренними документами МБОУ «СОШ №32 с углубленным изучением отдельных предметов», которые дополняют и уточняют ее.

Модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных МБОУ «Средняя общеобразовательная школа №32 с углубленным изучением отдельных предметов».

Модель угроз безопасности персональных данных (далее – Модель) при их обработке в информационной системе персональных данных (далее – ИСПДн):

1) «БАРС – Бюджет»
2) «Электронное образование в Республике Татарстан» (далее – «ЭО РТ»)
3) «Учет и мониторинг граждан, находящихся в социально-опасном положении» (далее – «СОП»)

включает:

- описание угроз.
- оценку вероятности возникновения угроз.
- оценку реализуемости угроз.
- оценку опасности угроз.
- определение актуальности угроз.

В заключении даны рекомендации по мерам защиты для уменьшения опасности актуальных угроз.

1.Описание угроз и оценка вероятности их возникновения

Классификация нарушителей

По признаку принадлежности к ИСПДн все нарушители делятся на две группы:

- *внешние нарушители* – физические лица, не имеющие права пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн;

- *внутренние нарушители* – физические лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн.

Внешний нарушитель

В качестве внешнего нарушителя информационной безопасности, рассматривается нарушитель, который не имеет непосредственного доступа к техническим средствам и ресурсам системы, находящимся в пределах контролируемой зоны.

Предполагается, что внешний нарушитель не может воздействовать на защищаемую информацию по техническим каналам утечки, так как объем информации, хранимой и обрабатываемой в ИСПДн, является недостаточным для возможной мотивации внешнего нарушителя к осуществлению действий, направленных на утечку информации по техническим каналам утечки.

Предполагается, что внешний нарушитель может воздействовать на защищаемую информацию только во время ее передачи по каналам связи.

Внутренний нарушитель

Возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны ограничительных факторов, из которых основным является реализация комплекса организационно-технических мер, в том числе по подбору, расстановке и обеспечению высокой профессиональной подготовки кадров, допуску физических лиц внутрь контролируемой зоны и контролю за порядком проведения работ, направленных на предотвращение и пресечение несанкционированного доступа.

Система разграничения доступа ИСПДн обеспечивает разграничение прав пользователей на доступ к информационным, программным, аппаратным и другим ресурсам ИСПДн в соответствии с принятой политикой информационной безопасности (правилами). К внутренним нарушителям могут относиться:

- администраторы ИСПДн (категория I);
- администраторы конкретных подсистем или баз данных ИСПДн (категория II);
- пользователи ИСПДн (категория III);
- пользователи, являющиеся внешними по отношению к конкретной автоматизированной системе (категория IV);
- лица, обладающие возможностью доступа к системе передачи данных (категория V);
- сотрудники учреждения, имеющие санкционированный доступ в служебных целях в помещения, в которых размещаются элементы ИСПДн, но не имеющие права доступа к ним (категория VI);
- обслуживающий персонал учреждения (категория VII);
- уполномоченный персонал разработчиков ИСПДн, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов ИСПДн (категория VIII).

На лиц категорий I и II возложены задачи по администрированию программно-аппаратных средств и баз данных ИСПДн для интеграции и обеспечения взаимодействия различных подсистем, входящих в состав ИСПДн. Администраторы потенциально могут реализовывать угрозы информационной безопасности (далее – ИБ), используя возможности по непосредственному доступу к защищаемой информации, обрабатываемой и хранимой в ИСПДн, а также к техническим и программным средствам ИСПДн, включая средства защиты, используемые в конкретных АС, в соответствии с установленными для них административными полномочиями.

Эти лица хорошо знакомы с основными алгоритмами, протоколами, реализуемыми и используемыми в конкретных подсистемах и ИСПДн в целом, а также с применяемыми принципами и концепциями безопасности.

Предполагается, что они могли бы использовать стандартное оборудование либо для идентификации уязвимостей, либо для реализации угроз ИБ. Данное оборудование может быть как частью штатных средств, так и может относиться к легко получаемому (например, программное обеспечение, полученное из общедоступных внешних источников).

Кроме того, предполагается, что эти лица могли бы располагать специализированным оборудованием.

К лицам категорий I и II ввиду их исключительной роли в ИСПДн должен применяться комплекс особых организационно-режимных мер по их подбору, принятию на работу, назначению на должность и контролю выполнения функциональных обязанностей.

Предполагается, что в число лиц категорий I и II будут включаться только доверенные лица и поэтому указанные лица исключаются из числа вероятных нарушителей.

Предполагается, что лица категорий III-VIII относятся к вероятным нарушителям.

Предполагается, что возможность сговора внутренних нарушителей маловероятна ввиду принятых организационных и контролирующих мер.

Предположения об имеющейся у нарушителя информации об объектах реализации угроз

В качестве основных уровней знаний нарушителей об АС можно выделить следующие:

- *общая информация* – информации о назначении и общих характеристиках ИСПДн;
- *эксплуатационная информация* – информация, полученная из эксплуатационной документации;
- *чувствительная информация* – информация, дополняющая эксплуатационную информацию об ИСПДн (например, сведения из проектной документации ИСПДн).

В частности, нарушитель может иметь:

- данные об организации работы, структуре и используемых технических, программных и программно-технических средствах ИСПДн;
- сведения об информационных ресурсах ИСПДн: порядок и правила создания, хранения и передачи информации, структура и свойства информационных потоков;
- данные об уязвимостях, включая данные о недокументированных (недекларированных) возможностях технических, программных и программно-технических средств ИСПДн;
- данные о реализованных в программных средствах защиты информации (далее – ПСЗИ) принципах и алгоритмах;
- исходные тексты программного обеспечения ИСПДн;
- сведения о возможных каналах реализации угроз;
- информацию о способах реализации угроз.

Предполагается, что лица категории III и категории IV владеют только эксплуатационной информацией, что обеспечивается организационными мерами. При этом лица категории IV не владеют парольной, аутентифицирующей и ключевой информацией, используемой в АИС, к которым они не имеют санкционированного доступа.

Предполагается, что лица категории V владеют в той или иной части чувствительной и эксплуатационной информацией о системе передачи информации и общей информацией об АИС, использующих эту систему передачи информации, что обеспечивается организационными мерами. При этом лица категории V не владеют парольной и аутентифицирующей информацией, используемой в АИС.

Предполагается, что лица категории VI и лица категории VII по уровню знаний не превосходят лица категории V.

Предполагается, что лица категории VIII обладают чувствительной информацией об

ИСПДн и функционально ориентированных АИС, включая информацию об уязвимостях технических и программных средств ИСПДн. Организационными мерами предполагается исключить доступ лиц категории VIII к техническим и программным средствам ИСПДн в момент обработки с использованием этих средств защищаемой информации.

Таким образом, наиболее информированными об АИС являются лица категории III и лица категории VIII.

Степень информированности нарушителя зависит от многих факторов, включая реализованные в ЛПУ конкретные организационные меры и компетенцию нарушителей. Поэтому объективно оценить объем знаний вероятного нарушителя в общем случае практически невозможно.

В связи с изложенным, с целью создания определенного запаса прочности предполагается, что вероятные нарушители обладают всей информацией, необходимой для подготовки и реализации угроз, за исключением информации, доступ к которой со стороны нарушителя исключается системой защиты информации. К такой информации, например, относится парольная, аутентифицирующая и ключевая информация.

Предположения об имеющихся у нарушителя средствах реализации угроз

Предполагается, что нарушитель имеет:

- аппаратные компоненты системы защиты персональных данных (далее – СЗПДн);
- доступные в свободной продаже технические средства и программное обеспечение;
- специально разработанные технические средства и программное обеспечение.

Внутренний нарушитель может использовать штатные средства.

Состав имеющихся у нарушителя средств, которые он может использовать для реализации угроз ИБ, а также возможности по их применению зависят от многих факторов, включая реализованные в учреждении конкретные организационные меры, финансовые возможности и компетенцию нарушителей. Поэтому объективно оценить состав имеющихся у нарушителя средств реализации угроз в общем случае практически невозможно.

Поэтому, для создания устойчивой СЗПДн предполагается, что вероятный нарушитель имеет все необходимые для реализации угроз средства, возможности которых не превосходят возможности аналогичных средств реализации угроз на информацию, содержащую сведения, составляющие государственную тайну, и технические и программные средства, обрабатывающие эту информацию.

Вместе с тем предполагается, что нарушитель не имеет:

- средств перехвата в технических каналах утечки;
- средств воздействия через сигнальные цепи;
- средств воздействия на источники и через цепи питания;
- средств воздействия через цепи заземления;
- средств активного воздействия на технические средства (средств облучения).

Предполагается, что наиболее совершенными средствами реализации угроз обладают лица категории III и лица категории VIII.

Угрозы утечки акустической (речевой) информации

Возникновение угроз утечки акустической (речевой) информации, содержащейся непосредственно в произносимой речи пользователя ИСПДн, при обработке персональных данных (далее – ПДн) в ИСПДн, возможно при наличием функций голосового ввода ПДн в ИСПДн или функций воспроизведения ПДн акустическими средствами ИСПДн.

В ИСПДн Учреждения функции голосового ввода ПДн или функции воспроизведения ПДн акустическими средствами отсутствуют.

Вероятность реализации угрозы – **маловероятна.**

Угрозы утечки видовой информации

Реализация угрозы утечки видовой информации возможна за счет просмотра информации с помощью оптических (оптико-электронных) средств с экранов дисплеев и других средств отображения средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав ИСПДн.

В учреждении введен контроль доступа в контролируемую зону, АРМ пользователей расположены так, что практически исключен визуальный доступ к мониторам, а на окнах установлены жалюзи.

Вероятность реализации угрозы – **маловероятна.**

Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок (далее – ПЭМИН)

Угрозы утечки информации по каналу ПЭМИН, возможны из-за наличия паразитных электромагнитных излучений у элементов ИСПДн.

Угрозы данного класса **маловероятны**, т.к. размер контролируемой зоны большой, и элементы ИСПДн, находятся в самом центре здания и экранируются несколькими несущими стенами, и паразитный сигнал маскируется со множеством других паразитных сигналов элементов, не входящих в ИСПДн.

Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн

Кража персональной электронной вычислительной машины (далее - ПЭВМ.)

Угроза осуществляется путем несанкционированного доступа (далее – НСД) внешними и внутренними нарушителями в помещения, где расположены элементы ИСПДн.

В учреждении введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок.

Вероятность реализации угрозы – **маловероятна.**

Кража носителей информации

Угроза осуществляется путем НСД внешними и внутренними нарушителями к носителям информации.

В Учреждении введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок.

Вероятность реализации угрозы – **маловероятна.**

Кража ключей и атрибутов доступа

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где происходит работа пользователей.

В Учреждении введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок.

Вероятность реализации угрозы – **маловероятна.**

Кражи, модификации, уничтожения информации

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены элементы ИСПДн и средства защиты, а так же происходит работа пользователей.

В Учреждении введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок.

Вероятность реализации угрозы – **маловероятна.**

Вывод из строя узлов ПЭВМ, каналов связи

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены элементы ИСПДн и проходят каналы связи.

В Учреждении введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок.

Вероятность реализации угрозы – **маловероятна.**

Несанкционированное отключение средств защиты

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены средства защиты ИСПДн.

В Учреждении введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок, пользователи ИСПДн проинструктированы о работе с ПДн.

Вероятность реализации угрозы – **маловероятна.**

Угрозы хищения, несанкционированной модификации или блокирования информации за счет НСД с применением программно-аппаратных и программных средств.

Действия вредоносных программ (вирусов).

Программно-математическое воздействие - это воздействие с помощью вредоносных программ. Программой с потенциально опасными последствиями или вредоносной программой (вирусом) называют некоторую самостоятельную программу (набор инструкций), которая способна выполнять любое непустое подмножество следующих функций:

- скрывать признаки своего присутствия в программной среде компьютера;
- обладать способностью к самодублированию, ассоциированию себя с другими программами и (или) переносу своих фрагментов в иные области оперативной или внешней памяти;
- разрушать (искажать произвольным образом) код программ в оперативной памяти;
- выполнять без инициирования со стороны пользователя (пользовательской программы в штатном режиме ее выполнения) деструктивные функции (копирования, уничтожения, блокирования и т.п.);
- сохранять фрагменты информации из оперативной памяти в некоторых областях внешней памяти прямого доступа (локальных или удаленных);
- искажать произвольным образом, блокировать и (или) подменять выводимый во внешнюю память или в канал связи массив информации, образовавшийся в результате работы прикладных программ, или уже находящиеся во внешней памяти массивы данных.

В Учреждении на всех элементах ИСПДн установлена антивирусная защита, пользователи проинструктированы о мерах предотвращения вирусного заражения.

Вероятность реализации угрозы – **низкая.**

Недекларированные возможности системного программного обеспечения (далее – ПО) и ПО для обработки персональных данных.

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

В Учреждении нет программного обеспечения разрабатываемого собственными разработчиками/сторонними специалистами.

Вероятность реализации угрозы – **маловероятна**.

Установка ПО не связанного с исполнением служебных обязанностей

Угроза осуществляется путем несанкционированной установки ПО внутренними нарушителями, что может привести к нарушению конфиденциальности, целостности и доступности всей ИСПДн или ее элементов.

В Учреждении осуществляется контроль по используемому ПО, пользователи проинструктированы о политике установки ПО.

Вероятность реализации угрозы – **низкая**.

Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от стихийного характера.

Утрата ключей и атрибутов доступа

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПДн, которые нарушают положения парольной политике в части их создания (создают легкие или пустые пароли, не меняют пароли по истечении срока их жизни или компрометации и т.п.) и хранения (записывают пароли на бумажные носители, передают ключи доступа третьим лицам и т.п.) или не осведомлены о них.

В Учреждении введена парольная политика, предусматривающая требуемую сложность пароля и периодическую его смену, введена политика «чистого стола», осуществляется контроль за их выполнением, пользователи проинструктированы о парольной политике и о действиях в случаях утраты или компрометации паролей.

Вероятность реализации угрозы – **низкая**.

Непреднамеренная модификация (уничтожение) информации сотрудниками

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПДн, которые нарушают положения принятых правил работы с ИСПДн или не осведомлены о них.

В Учреждении осуществляется резервное копирование обрабатываемых ПДн, пользователи проинструктированы о работе с ИСПДн.

Вероятность реализации угрозы – **маловероятна**.

Непреднамеренное отключение средств защиты

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПДн, которые нарушают положения принятых правил работы с ИСПДн и средствами защиты или не осведомлены о них.

В Учреждении введен контроль доступа в контролируемую зону, двери закрываются на замок, осуществляется разграничение доступа к настройкам режимов средств защиты, пользователи проинструктированы о работе с ИСПДн.

Вероятность реализации угрозы – **маловероятна**.

Выход из строя аппаратно-программных средств

Угроза осуществляется вследствие несовершенства аппаратно-программных средств, из-за которых может происходить нарушение целостности и доступности защищаемой информации.

В Учреждении осуществляет резервирование ключевых элементов ИСПДн.

Вероятность реализации угрозы – **маловероятна**.

Сбой системы электроснабжения

Угроза осуществляется вследствие несовершенства системы электроснабжения, из-за

чего может происходить нарушение целостности и доступности защищаемой информации.

В Учреждении осуществляет резервное копирование информации.

Вероятность реализации угрозы – **маловероятна.**

Стихийное бедствие

Угроза осуществляется вследствие несоблюдения мер пожарной безопасности.

В Учреждении установлена пожарная сигнализация, пользователи проинструктированы о действиях в случае возникновения внештатных ситуаций.

Вероятность реализации угрозы – **маловероятна.**

Угрозы преднамеренных действий внутренних нарушителей

Доступ к информации, модификация, уничтожение лиц, не допущенных к ее обработке

Угроза осуществляется путем НСД внешних нарушителей в помещения, где расположены элементы ИСПДн и средства защиты, а так же происходит работа пользователей.

В Учреждении введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок. Вероятность реализации угрозы – **маловероятна.**

Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПДн, которые нарушают положения о неразглашении обрабатываемой информации или не осведомлены о них.

В Учреждении пользователи осведомлены о порядке работы с персональными данными.

Вероятность реализации угрозы – **маловероятна.**

Угрозы несанкционированного доступа по каналам связи

Угроза «Анализ сетевого трафика»

Эта угроза реализуется с помощью специальной программы-анализатора пакетов (sniffer), перехватывающей все пакеты, передаваемые по сегменту сети, и выделяющей среди них те, в которых передаются идентификатор пользователя и его пароль. В ходе реализации угрозы нарушитель:

- изучает логику работы ИСПДн - то есть стремится получить однозначное соответствие событий, происходящих в системе, и команд, пересылаемых при этом хостами, в момент появления данных событий. В дальнейшем это позволяет злоумышленнику на основе задания соответствующих команд получить, например, привилегированные права на действия в системе или расширить свои полномочия в ней;
- перехватывает поток передаваемых данных, которыми обмениваются компоненты сетевой операционной системы, для извлечения конфиденциальной или идентификационной информации (например, статических паролей пользователей для доступа к удаленным хостам по протоколам FTP и TELNET, не предусматривающих шифрование), ее подмены, модификации и т.п.

Перехват за переделами с контролируемой зоны.

Вероятность реализации угрозы – **маловероятна.**

Перехват в пределах контролируемой зоны внешними нарушителями

В Учреждении введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок.

Вероятность реализации угрозы – **маловероятна.**

Перехват в пределах контролируемой зоны внутренними нарушителями.

В Учреждении введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок.

Вероятность реализации угрозы – **маловероятна.**

Угроза «сканирование сети»

Сущность процесса реализации угрозы заключается в передаче запросов сетевым службам хостов ИСПДн и анализе ответов от них. Цель - выявление используемых протоколов, доступных портов сетевых служб, законов формирования идентификаторов соединений, определение активных сетевых сервисов, подбор идентификаторов и паролей пользователей.

Вероятность реализации угрозы – **маловероятна.**

Угроза выявления паролей

Цель реализации угрозы состоит в получении НСД путем преодоления парольной защиты. Злоумышленник может реализовывать угрозу с помощью целого ряда методов, таких как простой перебор, перебор с использованием специальных словарей, установка вредоносной программы для перехвата пароля, подмена доверенного объекта сети (IP-spoofing) и перехват пакетов (sniffing). В основном для реализации угрозы используются специальные программы, которые пытаются получить доступ хосту путем последовательного подбора паролей. В случае успеха, злоумышленник может создать для себя «проход» для будущего доступа, который будет действовать, даже если на хосте изменить пароль доступа.

Вероятность реализации угрозы – **маловероятна.**

Угрозы навязывание ложного маршрута сети

Данная угроза реализуется одним из двух способов: путем внутрисегментного или межсегментного навязывания. Возможность навязывания ложного маршрута обусловлена недостатками, присущими алгоритмам маршрутизации (в частности из-за проблемы идентификации сетевых управляющих устройств), в результате чего можно попасть, например, на хост или в сеть злоумышленника, где можно войти в операционную среду технического средства в составе ИСПДн. Реализации угрозы основывается на несанкционированном использовании протоколов маршрутизации (RIP, OSPF, LSP) и управления сетью (ICMP, SNMP) для внесения изменений в маршрутно-адресные таблицы. При этом нарушителю необходимо послать от имени сетевого управляющего устройства (например, маршрутизатора) управляющее сообщение.

Вероятность реализации угрозы –**маловероятна.**

Угрозы подмены доверенного объекта

Такая угроза эффективно реализуется в системах, в которых применяются нестойкие алгоритмы идентификации и аутентификации хостов, пользователей и т.д. Под доверенным объектом понимается объект сети (компьютер, межсетевой экран, маршрутизатор и т.п.), легально подключенный к серверу.

Могут быть выделены две разновидности процесса реализации указанной угрозы: с установлением и без установления виртуального соединения.

Процесс реализации с установлением виртуального соединения состоит в присвоении прав доверенного субъекта взаимодействия, что позволяет нарушителю вести сеанс работы с объектом сети от имени доверенного субъекта. Реализация угрозы данного типа требует преодоления системы идентификации и аутентификации сообщений (например, атака rsh-

службы UNIX-хоста).

Процесс реализации угрозы без установления виртуального соединения может иметь место в сетях, осуществляющих идентификацию передаваемых сообщений только по сетевому адресу отправителя. Сущность заключается в передаче служебных сообщений от имени сетевых управляющих устройств (например, от имени маршрутизаторов) об изменении маршрутно-адресных данных.

В результате реализации угрозы нарушитель получает права доступа к техническому средству ИСПДн - цели угроз.

Вероятность реализации угрозы – **маловероятна.**

Внедрение ложного объекта сети

Эта угроза основана на использовании недостатков алгоритмов удаленного поиска. В случае если объекты сети изначально не имеют адресной информации друг о друге, используются различные протоколы удаленного поиска (например, SAP в сетях Novell NetWare; ARP, DNS, WINS в сетях со стеком протоколов TCP/IP), заключающиеся в передаче по сети специальных запросов и получении на них ответов с искомой информацией. При этом существует возможность перехвата нарушителем поискового запроса и выдачи на него ложного ответа, использование которого приведет к требуемому изменению маршрутно-адресных данных. В дальнейшем весь поток информации, ассоциированный с объектом-жертвой, будет проходить через ложный объект сети.

Вероятность реализации угрозы – **маловероятна.**

Угрозы типа «Отказ в обслуживании»

Эти угрозы основаны на недостатках сетевого программного обеспечения, его уязвимостях, позволяющих нарушителю создавать условия, когда операционная система оказывается не в состоянии обрабатывать поступающие пакеты.

Могут быть выделены несколько разновидностей таких угроз:

- скрытый отказ в обслуживании, вызванный привлечением части ресурсов ИСПДн на обработку пакетов, передаваемых злоумышленником со снижением пропускной способности каналов связи, производительности сетевых устройств, нарушением требований к времени обработки запросов. Примерами реализации угроз подобного рода могут служить: направленный шторм эхо-запросов по протоколу ICMP (Ping flooding), шторм запросов на установление TCP-соединений (SYN-flooding), шторм запросов к FTP-серверу;
- явный отказ в обслуживании, вызванный исчерпанием ресурсов ИСПДн при обработке пакетов, передаваемых злоумышленником (занятие всей полосы пропускания каналов связи, переполнение очередей запросов на обслуживание), при котором легальные запросы не могут быть переданы через сеть из-за недоступности среды передачи, либо получают отказ в обслуживании ввиду переполнения очередей запросов, дискового пространства памяти и т.д. Примерами угроз данного типа могут служить шторм широковещательных ICMP-эхо-запросов (Smurf), направленный шторм (SYN-flooding), шторм сообщений почтовому серверу (Spam);
- явный отказ в обслуживании, вызванный нарушением логической связности между техническим средствами ИСПДн при передаче нарушителем управляющих сообщений от имени сетевых устройств, приводящих к изменению маршрутно-адресных данных (например, ICMP Redirect Host, DNS-flooding) или идентификационной и аутентификационной информации;
- явный отказ в обслуживании, вызванный передачей злоумышленником пакетов с нестандартными атрибутами (угрозы типа «Land», «TearDrop», «Bonk», «Nuke», «UDP-bomb») или имеющих длину, превышающую максимально допустимый размер (угроза типа «Ping Death»), что может привести к сбою сетевых устройств, участвующих в обработке запросов, при условии наличия ошибок в программах, реализующих протоколы сетевого обмена.

Результатом реализации данной угрозы может стать нарушение работоспособности соответствующей службы предоставления удаленного доступа к ПДн в ИСПДн, передача с одного адреса такого количества запросов на подключение к техническому средству в составе ИСПДн, которое максимально может «вместить» трафик (направленный «шторм запросов»), что влечет за собой переполнение очереди запросов и отказ одной из сетевых служб или полная остановка ИСПДн из-за невозможности системы заниматься ничем другим, кроме обработки запросов.

Вероятность реализации угрозы – **маловероятна.**

Угрозы удаленного запуска приложений

Угроза заключается в стремлении запустить на хосте ИСПДн различные предварительно внедренные вредоносные программы: программы-закладки, вирусы, «сетевые шпионы», основная цель которых - нарушение конфиденциальности, целостности, доступности информации и полный контроль за работой хоста. Кроме того, возможен несанкционированный запуск прикладных программ пользователей для несанкционированного получения необходимых нарушителю данных, для запуска управляемых прикладной программой процессов и др.

Выделяют три подкласса данных угроз:

- распространение файлов, содержащих несанкционированный исполняемый код;
- удаленный запуск приложения путем переполнения буфера приложений-серверов;
- удаленный запуск приложения путем использования возможностей удаленного управления системой, предоставляемых скрытыми программными и аппаратными закладками, либо используемыми штатными средствами.

Типовые угрозы первого из указанных подклассов основываются на активизации распространяемых файлов при случайном обращении к ним. Примерами таких файлов могут служить: файлы, содержащие исполняемый код в вид документы, содержащие исполняемый код в виде элементов ActiveX, Java-апплетов, интерпретируемых скриптов (например, тексты на JavaScript); файлы, содержащие исполняемые коды программ. Для распространения файлов могут использоваться службы электронной почты, передачи файлов, сетевой файловой системы.

При угрозах второго подкласса используются недостатки программ, реализующих сетевые сервисы (в частности, отсутствие контроля за переполнением буфера). Настройкой системных регистров иногда удается переключить процессор после прерывания, вызванного переполнением буфера, на исполнение кода, содержащегося за границей буфера. Примером реализации такой угрозы может служить внедрение широко известного «вируса Морриса».

При угрозах третьего подкласса нарушитель использует возможности удаленного управления системой, предоставляемые скрытыми компонентами (например, «троянскими» программами типа Back. Orifice, Net Bus), либо штатными средствами управления и администрирования компьютерных сетей (Landesk Management Suite, Managewise, Back Orifice и т. п.). В результате их использования удается добиться удаленного контроля над станцией в сети.

Вероятность реализации угрозы – **маловероятна.**

Угрозы внедрения по сети вредоносных программ

К вредоносным программам, внедряемым по сети, относятся вирусы, которые для своего распространения активно используют протоколы и возможности локальных и глобальных сетей. Основным принципом работы сетевого вируса является возможность самостоятельно передать свой код на удаленный сервер или рабочую станцию. «Полноценные» сетевые вирусы при этом обладают еще и возможностью запустить на выполнение свой код на удаленном компьютере или, по крайней мере, «подтолкнуть» пользователя к запуску зараженного файла.

Вредоносными программами, обеспечивающими осуществление НСД, могут быть:

- программы подбора и вскрытия паролей;

- программы, реализующие угрозы;

- программы, демонстрирующие использование недекларированных возможностей программного и программно-аппаратного обеспечения ИСПДн;

- программы-генераторы компьютерных вирусов;

- программы, демонстрирующие уязвимости средств защиты информации и др.

Вероятность реализации угрозы – **маловероятна.**

2. Исходный уровень защищенности ИСПДн

Под общим уровнем защищенности понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн (Y1).

Числовой коэффициент (Y1) для оценки вероятности возникновения угрозы определяется по 4 вербальным градациям этого показателя:

- **маловероятно** - отсутствуют объективные предпосылки для осуществления угрозы (Y1 = 0);

- **низкая вероятность** - объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (Y1 = 2);

- **средняя вероятность** - объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны (Y1 = 5);

- **высокая вероятность** - объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты (Y1 = 10).

В таблице представлены характеристики уровня исходной защищенности для ИСПДн организации.

Таблица 1 – Исходный уровень защищенности

№ п/п	Технические и эксплуатационные характеристики	Уровень защищенности		
		ИСПДн «БАРС – Бюджет»	**ИСПДн «ЭО РТ»**	**ИСПДн «СОП»**
1	По территориальному размещению	0	0	0
2	По наличию соединения с сетями общего пользования	5	5	5
3	По встроенным (легальным) операциям с записями баз персональных данных	0	0	0
4	По разграничению доступа к персональным данным	0	0	0
5	По наличию соединений с другими базами ПДн иных ИСПДн	0	0	0
6	По уровню (обезличивания) ПДн	5	5	5
7	По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без	0	0	0

	предварительной обработки			

3. Вероятность реализации УБПДн

Под вероятностью реализации угрозы понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для ИСПДн в складывающихся условиях обстановки.

Числовой коэффициент (Y2) для оценки вероятности возникновения угрозы определяется по 4 вербальным градациям этого показателя:

- **маловероятно** - отсутствуют объективные предпосылки для осуществления угрозы (Y2 = 0);
- **низкая вероятность** - объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (Y2 = 2);
- **средняя вероятность** - объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны (Y2 = 5);
- **высокая вероятность** - объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты (Y2 = 10).

При обработке персональных данных в ИСПДн можно выделить следующие угрозы:

4. Реализуемость угроз

По итогам оценки уровня защищенности (Y1) и вероятности реализации угрозы (Y2), рассчитывается коэффициент реализуемости угрозы (Y) и определяется возможность реализации угрозы. Коэффициент реализуемости угрозы Y будет определяться соотношением Y = (Y1 + Y2)/20. Оценка реализуемости УБПДн представлена в таблице.

Таблица 2 – Реализуемость УБПДн

Тип угроз безопасности ПДн	Коэффициент реализуемости угрозы (Y)	Возможность реализации
1. Угрозы от утечки по техническим каналам.		
1.1. Угрозы утечки акустической информации	0	низкая
1.2. Угрозы утечки видовой информации	0	низкая
1.3. Угрозы утечки информации по каналам ПЭМИН	0	низкая
2. Угрозы несанкционированного доступа к информации.		
2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн		
2.1.1. Кража ПЭВМ	0	низкая

2.1.2. Кража носителей информации	0	низкая
2.1.3. Кража ключей и атрибутов доступа	0	низкая
2.1.4. Кражи, модификации, уничтожения информации	0	низкая
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	0,3	средняя
2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	0	низкая
2.1.7. Несанкционированное отключение средств защиты	0	низкая
2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий).		
2.2.1. Действия вредоносных программ (вирусов)	0,3	средняя
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных	0	низкая
2.2.3. Установка ПО не связанного с исполнением служебных обязанностей	0	низкая
2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.		
2.3.1. Утрата ключей и атрибутов доступа	0	низкая
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками	0,3	средняя
2.3.3. Непреднамеренное отключение средств защиты	0,3	средняя
2.3.4. Выход из строя аппаратно-программных средств	0,3	средняя
2.3.5. Сбой системы электроснабжения	0,3	средняя
2.3.6. Стихийное бедствие	0	низкая
2.4. Угрозы преднамеренных действий внутренних нарушителей		
2.4.1. Доступ к информации, модификация, уничтожение лиц не допущенных к ее обработке	0	низкая
2.4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее	0	низкая

обработке		
2.5.Угрозы несанкционированного доступа по каналам связи.		
2.5.1.Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:	0	низкая
2.5.1.1. Перехват за переделами с контролируемой зоны	0	низкая
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями	0	низкая
2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями.	0	низкая
2.5.2.Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	0	низкая
2.5.3.Угрозы выявления паролей по сети	0	низкая
2.5.4.Угрозы навязывание ложного маршрута сети	0	низкая
2.5.5.Угрозы подмены доверенного объекта в сети	0	низкая
2.5.6.Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	0	низкая
2.5.7.Угрозы типа «Отказ в обслуживании»	0	низкая
2.5.8.Угрозы удаленного запуска приложений	0	низкая
2.5.9.Угрозы внедрения по сети вредоносных программ	0	низкая

5. Оценка опасности угроз

Оценка опасности УБПДн производится на основе опроса специалистов по защите информации и определяется вербальным показателем опасности, который имеет три значения:

- **низкая опасность** - если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;
- **средняя опасность** - если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;
- **высокая опасность** - если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

Оценка опасности УБПДн представлена таблице.

Таблица 3 – Опасность УБПДн

Тип угроз безопасности ПДн	**Опасность угрозы**
1. Угрозы от утечки по техническим каналам.	
1.1. Угрозы утечки акустической информации	низкая опасность
1.2. Угрозы утечки видовой информации	низкая опасность
1.3. Угрозы утечки информации по каналам ПЭМИН	низкая опасность
2. Угрозы несанкционированного доступа к информации.	
2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн	
2.1.1. Кража ПЭВМ	низкая опасность
2.1.2. Кража носителей информации	низкая опасность
2.1.3. Кража ключей и атрибутов доступа	низкая опасность
2.1.4. Кражи, модификации, уничтожения информации	низкая опасность
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	низкая опасность
2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	средняя опасность
2.1.7. Несанкционированное отключение средств защиты	средняя опасность
2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий).	
2.2.1. Действия вредоносных программ (вирусов)	средняя опасность
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных	низкая опасность
2.2.3. Установка ПО не связанного с исполнением служебных обязанностей	низкая опасность
2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.	

2.3.1. Утрата ключей и атрибутов доступа	низкая опасность
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками	средняя опасность
2.3.3. Непреднамеренное отключение средств защиты	средняя опасность
2.3.4. Выход из строя аппаратно-программных средств	средняя опасность
2.3.5. Сбой системы электроснабжения	средняя опасность
2.3.6. Стихийное бедствие	низкая опасность
2.4. Угрозы преднамеренных действий внутренних нарушителей	
2.4.1. Доступ к информации, модификация, уничтожение лиц не допущенных к ее обработке	низкая опасность
2.4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке	низкая опасность
2.5.Угрозы несанкционированного доступа по каналам связи.	
2.5.1.Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:	низкая опасность
2.5.1.1. Перехват за переделами с контролируемой зоны	низкая опасность
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями	низкая опасность
2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями.	низкая опасность
2.5.2.Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	низкая опасность
2.5.3.Угрозы выявления паролей по сети	низкая опасность
2.5.4.Угрозы навязывание ложного маршрута сети	низкая опасность
2.5.5.Угрозы подмены доверенного объекта в сети	низкая опасность
2.5.6.Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	низкая опасность
2.5.7.Угрозы типа «Отказ в обслуживании»	низкая опасность
2.5.8.Угрозы удаленного запуска приложений	низкая опасность
2.5.9.Угрозы внедрения по сети вредоносных программ	низкая опасность

6. Определение актуальности угроз в ИСПДн

В соответствии с правилами отнесения угрозы безопасности к актуальной, для ИСПДн определяются актуальные и неактуальные угрозы.

Таблица 4 – Правила определения актуальности УБПДн

Возможность реализации угрозы	**Показатель опасности угрозы**		
	Низкая	**Средняя**	**Высокая**
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

Оценка актуальности угроз безопасности представлена в таблице.

Таблица 5 – Актуальность УБПДн

Тип угроз безопасности ПДн	**Опасность угрозы**
1. Угрозы от утечки по техническим каналам.	
1.1. Угрозы утечки акустической информации	неактуальная
1.2. Угрозы утечки видовой информации	неактуальная
1.3. Угрозы утечки информации по каналам ПЭМИН	неактуальная
2. Угрозы несанкционированного доступа к информации.	
2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн	
2.1.1. Кража ПЭВМ	неактуальная
2.1.2. Кража носителей информации	неактуальная
2.1.3. Кража ключей и атрибутов доступа	неактуальная
2.1.4. Кражи, модификации, уничтожения информации	неактуальная
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	неактуальная

2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	неактуальная
2.1.7. Несанкционированное отключение средств защиты	неактуальная
2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий).	
2.2.1. Действия вредоносных программ (вирусов)	актуальная
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных	неактуальная
2.2.3. Установка ПО не связанного с исполнением служебных обязанностей	неактуальная
2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.	
2.3.1. Утрата ключей и атрибутов доступа	неактуальная
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками	актуальная
2.3.3. Непреднамеренное отключение средств защиты	актуальная
2.3.4. Выход из строя аппаратно-программных средств	актуальная
2.3.5. Сбой системы электроснабжения	неактуальная
2.3.6. Стихийное бедствие	неактуальная
2.4. Угрозы преднамеренных действий внутренних нарушителей	
2.4.1. Доступ к информации, модификация, уничтожение лиц не допущенных к ее обработке	неактуальная
2.4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке	актуальная
2.5.Угрозы несанкционированного доступа по каналам связи.	
2.5.1.Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:	неактуальная
2.5.1.1. Перехват за переделами с контролируемой зоны	неактуальная
2.5.1.2. Перехват в пределах контролируемой зоны внешними	неактуальная

нарушителями	
2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями.	неактуальная
2.5.2.Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	неактуальная
2.5.3.Угрозы выявления паролей по сети	неактуальная
2.5.4.Угрозы навязывание ложного маршрута сети	неактуальная
2.5.5.Угрозы подмены доверенного объекта в сети	неактуальная
2.5.6.Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	неактуальная
2.5.7.Угрозы типа «Отказ в обслуживании»	неактуальная
2.5.8.Угрозы удаленного запуска приложений	неактуальная
2.5.9.Угрозы внедрения по сети вредоносных программ	неактуальная

7. Заключение

Были выявлены следующие актуальные угрозы:

1) Действия вредоносных программ (вирусов)
2) Непреднамеренная модификация (уничтожение) информации сотрудниками
3) Непреднамеренное отключение средств защиты
4) Выход из строя аппаратно-программных средств
5) Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке

Для снижения опасности реализации актуальных УБПДн рекомендуется осуществить следующие мероприятия:

1) Провести обучение сотрудников, допущенных к обработке ПДн правилам обращения с ПДн, требованиям нормативных документов.
2) Разработать инструкции пользователей ИСПДн.
3) Своевременно производить профилактическое обслуживание технических средств ИСПДн.
4) При расширении и модернизации ИСПДн учитывать актуальность возникновения угроз безопасности ПДн.

УТВЕРЖДАЮ
директор МБОУ «СОШ №32 с уиоп»
_____Рагузина В.И

«29» августа 2017 г.

ИНСТРУКЦИЯ
Администратора информационной безопасности информационных систем персональных данных Муниципального бюджетного образовательного учреждения «Средняя общеобразовательная школа №32 с углубленным изучением отдельных предметов»

1. Общие положения

Администратор информационной безопасности (далее - ИБ) информационной системы персональных данных (далее - ИСПДн) Муниципального бюджетного образовательного учреждения «Средняя общеобразовательная школа №32 с углубленным изучением отдельных предметов» (далее – МБОУ «СОШ №32 с углубленным изучением отдельных предметов») назначается приказом МБОУ «СОШ №32 с углубленным изучением отдельных предметов» и функционально подчиняется Рагузиной В.И., директору школы.

Администратор ИБ ИСПДн руководствуется требованиями нормативных документов Российской Федерации, нормативных актов МБОУ «СОШ №32 с углубленным изучением отдельных предметов», настоящей Инструкцией, а также другими распорядительными документами в части, его касающейся.

Администратор ИБ ИСПДн в пределах своих функциональных обязанностей обеспечивает работоспособность ИСПДн, безопасность информации, обрабатываемой, передаваемой и хранимой при помощи средств вычислительной техники (далее - СВТ) в ИСПДн МБОУ «СОШ №32 с углубленным изучением отдельных предметов»

Должностные лица МБОУ «СОШ №32 с углубленным изучением отдельных предметов», задействованные в обеспечении функционирования ИСПДн, могут быть ознакомлены с основными положениями и приложениями Инструкции в части, их касающейся, по мере необходимости.

В случае увольнения администратор ИБ ИСПДн МБОУ «СОШ №32 с углубленным изучением отдельных предметов» обязан передать руководителю МБОУ «СОШ №32 с углубленным изучением отдельных предметов» все носители защищаемой информации МБОУ «СОШ №32 с углубленным изучением отдельных предметов» (рукописи, черновики, чертежи, диски, дискеты, распечатки с принтеров, модели, материалы, изделия и пр.), которые находились в его распоряжении в связи с выполнением им служебных обязанностей во время работы в МБОУ «СОШ №32 с углубленным изучением отдельных предметов»

2. Обязанности администратора ИБ ИСПДН

Администратор ИБ ИСПДн обязан:

- знать перечень установленных в подразделении СВТ и перечень задач, решаемых с их использованием;
- обеспечивать работоспособность средств вычислительной техники ИСПДн МБОУ «СОШ №32 с углубленным изучением отдельных предметов», проводить организационно-технические мероприятия по их обслуживанию;
- устанавливать и настраивать элементы ИСПДн и средства защиты информации, а также выполнять другие возложенные на него работы в соответствии с распорядительными, инструктивными и методическими материалами в части, его касающейся;
- рассматривать целесообразность применения новых технологий для повышения эффективности функционирования ИСПДн МБОУ «СОШ №32 с углубленным изучением отдельных предметов»;
- подготавливает обоснования и спецификации для закупки, заказывает новые элементы ИСПДн и расходные материалы;
- поддерживает резерв расходных материалов;
- изучает рынок программных средств и предоставляет рекомендации по приобретению и внедрению системного и прикладного программного обеспечения; - выполнять своевременное обновление программного обеспечения элементов ИСПДн и средств защиты персональных данных (СЗПДн) по мере появления таких обновлений;
- выполнять резервное копирование и восстановление данных;
- обеспечивать контроль за выполнением пользователями требований «Инструкции пользователю ИСПДн»;
- осуществлять контроль за работой пользователей автоматизированных систем, выявление попыток НСД к защищаемым информационным ресурсам и техническим средствам ИСПДн МБОУ «СОШ №32 с углубленным изучением отдельных предметов»;
- осуществлять настройку средств защиты, выполнять другие действия по изменению элементов ИСПДн;
- осуществлять учет всех защищаемых носителей информации с помощью их любой маркировки и с занесением учетных данных в специальный журнал (учетную карточку). Учтенные носители информации выдавать пользователям под роспись;
- осуществлять текущий и периодический контроль работы средств и систем защиты информации;
- осуществлять текущий контроль технологического процесса обработки защищаемой информации;
- периодически осуществлять тестирование всех функций системы защиты с помощью тестовых программ, имитирующих попытки НСД, при изменении программной среды и персонала ИСПДн;

- в случае возникновения нештатных ситуаций (сбоев в работе СЗПДн) немедленно докладывать ответственному за обеспечение безопасности ПДн;

- участвовать в проведении служебных расследований фактов нарушения или угрозы нарушения безопасности защищаемой информации;

- участвовать в проведении работ по восстановлению работоспособности средств и систем защиты информации;

- вести «Журнал учета нештатных ситуаций», учитывать факты вскрытия и опечатывания ПЭВМ, выполнения профилактических работ, установки и модификации аппаратных и программных средств ПЭВМ. Форма журнала приведена в «Инструкции по действиям персонала в нештатных ситуациях»;

- проводить обучение персонала и пользователей вычислительной техники правилам работы с СВТ и средствами защиты информации с отметкой в карточке инструктажа (Приложение 2);

- участвовать в разработке нормативных и методических материалов, связанных с функционированием СВТ и применением средств защиты информации, выполнением мероприятий по обеспечению защиты информации; - регулярно анализировать работу любых элементов АС, электронных системных журналов средств защиты для выявления и устранения неисправностей, а также для оптимизации ее функционирования.

3. Права администратора ИБ ИСПДН

Администратор ИБ ИСПДн имеет право:

- отключать любые элементы СЗПДн при изменении конфигурации, регламентном техническом обслуживании или устранении неисправностей в установленном порядке;

- в установленном порядке изменять конфигурацию элементов ИСПДн и СЗПДн;

- требовать от сотрудников МБОУ «СОШ №32 с углубленным изучением отдельных предметов» соблюдения правил работы в ИСПДн, приведенных в «Инструкции пользователя ИСПДн»;

- требовать от пользователей безусловного соблюдения установленной технологии обработки защищаемой информации и выполнения требований внутренних документов МБОУ «СОШ №32 с углубленным изучением отдельных предметов», регламентирующих вопросы обеспечения безопасности и защиты информации;

- обращаться к ответственному за обеспечение безопасности ПДн с требованием о прекращении обработки информации в случаях нарушения установленной технологии обработки защищаемой информации или нарушения функционирования средств и систем защиты информации;

- вносить свои предложения по совершенствованию функционирования ИСПДн - Учет и мониторинг граждан, находящихся в социально – опасном положении ;

- Электронное образование в Республике Татарстан;

- Барс – Бюджет

- инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения информационной безопасности в ИСПДн - Учет и мониторинг граждан, находящихся в социально – опасном положении ;

- Электронное образование в Республике Татарстан;

- Барс – Бюджет

Ответственность администратора ИБ ИСПДН

Администратор ИБ ИСПДн несет ответственность:

- за ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей инструкцией, другими инструктивными документами в

соответствии с действующим законодательством Российской Федерации, за полноту и качество проводимых им работ по обеспечению защиты информации;

- за правонарушения, совершенные в процессе своей деятельности в пределах, определенных действующим законодательством Российской Федерации;
- за разглашение сведений конфиденциального характера и другой защищаемой информации МБОУ «СОШ №32 с углубленным изучением отдельных предметов» в пределах, определенных действующим законодательством Российской Федерации;
- на администратора ИБ ИСПДн возлагается персональная ответственность за работоспособность и надлежащее функционирование средств обработки ПДн в ИСПДн и средств защиты персональных данных МБОУ «СОШ №32 с углубленным изучением отдельных предметов»

4. Порядок пересмотра инструкции

Инструкция подлежит полному пересмотру при изменении перечня решаемых задач, состава технических и программных средств ИСПДн

- Учет и мониторинг граждан, находящихся в социально – опасном положении ;
- Электронное образование в Республике Татарстан;
- Барс – Бюджет**,** приводящих к существенным изменениям технологии обработки информации.

Инструкция подлежит частичному пересмотру в остальных случаях. Частичный пересмотр проводится ответственным за обеспечение безопасности ПДн МБОУ «СОШ №32 с углубленным изучением отдельных предметов»

Полный пересмотр данного документа проводится ответственным за обеспечение безопасности ПДн МБОУ «СОШ №32 с углубленным изучением отдельных предметов» с целью проверки соответствия положений данного документа реальным условиям применения их в ИСПДн

- Учет и мониторинг граждан, находящихся в социально – опасном положении ;
- Электронное образование в Республике Татарстан;
- Барс – Бюджет

Форма регистрации изменений в Инструкцию представлена в Приложении 3.

Вносимые изменения не должны противоречить другим положениям Инструкции.

1. ОТВЕТСТВЕННЫЕ ЗА КОНТРОЛЬ ВЫПОЛНЕНИЯ ИНСТРУКЦИИ

Ответственным за контроль выполнения требований данной Инструкции является ответственный за обеспечение безопасности ПДн.

ПРИЛОЖЕНИЕ 1.
КАРТОЧКА ИНСТРУКТАЖА

КАРТОЧКА № ____ ПРОВЕДЕНИЯ ИНСТРУКТАЖА ПО ВОПРОСАМ ЗАЩИТЫ ИНФОРМАЦИИ

Учреждение		
Дата		
Фамилия, инициалы инструктируемого	Должность	Роспись
Вид инструктажа (в связи с чем проводится)		
Краткое содержание инструктажа		
Инструктаж провел Администратор ИБ ИСПДн:		

Примечание: Заполненная карточка хранится у Администратора ИБ ИСПДн.

ПРИЛОЖЕНИЕ 2.
ФОРМА РЕГИСТРАЦИИ ИЗМЕНЕНИЙ В ИНСТРУКЦИЮ

ЛИСТ
регистрации изменений в инструкции

№ п.п.	Дата	Внесенное изменение	Основание (наименование, номер и дата документа)	Кем внесено изменение (должность, подпись)

ПРИЛОЖЕНИЕ 3

ЛИСТ ОЗНАКОМЛЕНИЯ
с инструкцией администратора информационной безопасности информационных систем персональных данных МБОУ «СОШ №32 с углубленным изучением отдельных предметов»

№ п/п	Фамилия, инициалы сотрудника	Дата ознакомления	Расписка сотрудника в ознакомлении

УТВЕРЖДАЮ
директор МБОУ «СОШ №32 с уиоп»
_____Рагузина В.И

«29» августа 2017 г.

ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Настоящий документ подготовлен в рамках выполнения работ по обеспечению безопасной эксплуатации информационных систем персональных данных:

- Учет и мониторинг граждан, находящихся в социально – опасном положении ;
- Электронное образование в Республике Татарстан;
- Барс – Бюджет

(далее - ИСПДн).

1. Общие положения

1.1. Пользователь ИСПДн (далее - Пользователь) осуществляет обработку персональных данных в ИСПДн

- Учет и мониторинг граждан, находящихся в социально – опасном положении ;
- Электронное образование в Республике Татарстан;
- Барс – Бюджет

(далее – *СОП, ЭО, Барс-бюджет*).

1.2. Пользователем является каждый работник Муниципального бюджетного образовательного учреждения «Средняя общеобразовательная школа №32 с углубленным изучением отдельных предметов» (далее - МБОУ «СОШ №32 с углубленным изучением отдельных предметов», участвующий в рамках своих функциональных обязанностей в

процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.

1.3. Пользователь несет персональную ответственность за свои действия.

1.4. Пользователь в своей работе руководствуется настоящей Инструкцией, и другими регламентирующими документами *МБОУ «СОШ №32 с углубленным изучением отдельных предметов»*.

2. Должностные обязанности

Пользователь обязан:

2.1. Знать и выполнять требования настоящей Инструкции и других внутренних распоряжений, регламентирующих порядок действий по защите персональных данных.

2.2. Выполнять на автоматизированном рабочем месте (далее - АРМ) только те процедуры обработки персональных данных, которые определены для него должностной инструкцией.

2.3. Знать и соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и пересылке носителей информации, обеспечению безопасности ПДн, а также руководящих и организационно-распорядительных документов.

2.4. Соблюдать требования парольной политики.

2.5. Соблюдать правила при работе в сетях общего доступа и (или) международного обмена - Интернет и других.

2.6. Обо всех выявленных нарушениях, связанных с информационной безопасностью МБОУ «СОШ №32 с углубленным изучением отдельных предметов», а также для получения консультаций по вопросам информационной безопасности необходимо обратиться к ответственному за организацию работы с ПД Баринову Е.Г..

2.7. Пользователям запрещается:

разглашать защищаемую информацию третьим лицам;

копировать защищаемую информацию на внешние носители без разрешения своего руководителя;

самостоятельно устанавливать, тиражировать или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;

несанкционированно открывать общий доступ к папкам на своей рабочей станции;

отключать (блокировать) средства защиты информации;

обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к ИСПДн;

сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн;

привлекать посторонних лиц для производства ремонта или настройки АРМ без согласования с ответственным за организацию работы с ПД.

2.8. При отсутствии визуального контроля за рабочей станцией доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию <Блокировка>.

2.9. Принимать меры по реагированию в случае возникновения внештатных ситуаций и аварийных ситуаций с целью ликвидации их последствий в пределах возложенных на него функций.

3. Организация парольной защиты

3.1. Полная плановая смена паролей в ИСПДн проводится не реже одного раза в 3 месяца.

3.2. Правила формирования пароля:

- пароль не может содержать имя учетной записи пользователя или какую-либо его часть;
- пароль должен состоять не менее чем из 8 символов;
- в пароле должны присутствовать символы трех категорий из числа следующих четырех:

а) прописные буквы английского алфавита от A до Z;

б) строчные буквы английского алфавита от a до z;

в) десятичные цифры (от 0 до 9);

г) символы, не принадлежащие алфавитно-цифровому набору (например, !, $, #, %);

- запрещается использовать в качестве пароля имя входа в систему, простые пароли типа "123", "111", "qwerty" и им подобные, а также имена и даты рождения своей личности и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о пользователе;
- запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;
- запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);
- запрещается выбирать пароли, которые уже использовались ранее.

3.3. Правила ввода пароля:

ввод пароля должен осуществляться с учетом регистра, в котором пароль был задан;

во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамерами и др.).

3.4. Правила хранения пароля:

запрещается записывать пароли на бумаге, в файле, в электронной записной книжке и на других носителях информации, в том числе на предметах;

запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

3.5. Лица, использующие паролирование, обязаны:

четко знать и строго выполнять требования настоящей Инструкции и других руководящих документов по паролированию;

своевременно сообщать ответственным за организацию работы с ПД об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

4. Правила работы в сетях общего доступа и (или) международного обмена

4.1. Работа в сетях общего доступа и (или) международного обмена (сети "Интернет" и других) (далее - Сеть) на элементах ИСПДн должна проводиться при служебной необходимости.

4.2. При работе в Сети запрещается:

осуществлять работу при отключенных средствах защиты (антивирусах и других);

передавать по Сети защищаемую информацию без использования средств шифрования;

посещать сайты сомнительной репутации (порносайты, сайты, содержащие нелегально распространяемое ПО, и другие).

УТВЕРЖДАЮ
директор МБОУ «СОШ №32 с уиоп»
_____Рагузина В.И.
29 августа 2017 г.

Инструкция по организации антивирусной защиты информационных систем персональных данных

Муниципального бюджетного образовательного учреждения
«Средняя общеобразовательная школа №32
с углубленным изучением отдельных предметов»

Общие положения

1.1. Инструкция по организации антивирусной защиты информационных систем персональных данных Муниципального бюджетного образовательного учреждения «Средняя общеобразовательная школа №32 с углубленным изучением отдельных предметов» (далее – МБОУ «СОШ №32 с углубленным изучением отдельных предметов») определяет требования к организации защиты информационных систем персональных данных (далее - ИСПДн) от разрушающего воздействия компьютерных вирусов и другого вредоносного программного обеспечения (далее - ПО) и устанавливает ответственность руководителей и сотрудников МБОУ «СОШ №32 с углубленным изучением отдельных предметов», эксплуатирующих и сопровождающих ИСПДн, за их выполнение.

1.2. Требования настоящей Инструкции распространяются на всех должностных лиц и сотрудников МБОУ «СОШ №32 с углубленным изучением отдельных предметов», использующих в работе ИСПДн

- Учет и мониторинг граждан, находящихся в социально – опасном положении ;
- Электронное образование в Республике Татарстан;
- Барс – Бюджет

1.3. В целях закрепления знаний по вопросам практического исполнения требований Инструкции, разъяснения возникающих вопросов, проводятся организуемые Администратором

безопасности ИСПДн семинары и персональные инструктажи (при необходимости) пользователей ИСПДн

- Учет и мониторинг граждан, находящихся в социально – опасном положении ;
- Электронное образование в Республике Татарстан;
- Барс – Бюджет

1.4. Доведение Инструкции до сотрудников МБОУ «СОШ №32 с углубленным изучением отдельных предметов» в части их касающейся осуществляется Администратором безопасности ИСПДн под роспись в журнале или на самом документе.

1.5. В случае невозможности исполнения требований настоящей Инструкции в полном объеме, например: − в нештатных ситуациях, возникающих вследствие отказов, сбоев, ошибок, стихийных бедствий, побочных влияний; − злоумышленных действий, практическая «глубина» исполнения настоящей Инструкции определяется Администратором безопасности ИСПДн по согласованию с ответственным за обеспечение безопасности ПДн МБОУ «СОШ №32 с углубленным изучением отдельных предметов».

Применение средств антивирусной защиты

2.1. Антивирусный контроль дисков и файлов ИСПДн после загрузки компьютера должен проводиться в автоматическом режиме (периодическое сканирование или мониторинг).

2.2. Периодически, не реже одного раза в месяц, должен проводиться полный антивирусный контроль всех дисков и файлов ИСПДн (сканирование).

2.3. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая информация по телекоммуникационным каналам связи, на съемных носителях (магнитных дисках, CD-ROM и т.п.). Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема. Контроль исходящей информации необходимо проводить непосредственно перед отправкой (записью на съемный носитель).

2.4. Установка (обновление и изменение) системного и прикладного программного обеспечения осуществляется в соответствии с «Инструкцией по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств ИСПДн

- Учет и мониторинг граждан, находящихся в социально – опасном положении ;
- Электронное образование в Республике Татарстан;
- Барс – Бюджет

2.5. Обновление антивирусных баз должно проводиться регулярно, но не реже, чем 1 раз в неделю.

Функции администратора ИСПДН по обеспечению антивирусной безопасности

Администратор безопасности ИСПДн обязан:

3.1. При необходимости проводить инструктажи пользователей ИСПДн по вопросам применения средств антивирусной защиты.

3.2. Настраивать параметры средств антивирусного контроля в соответствии с руководствами по применению конкретных антивирусных средств.

3.3. Предварительно проверять устанавливаемое (обновляемое) программное обеспечение на отсутствие вирусов.

3.4. При необходимости производить обновление антивирусных программных средств.

3.5. Производить получение и рассылку (при необходимости) обновлений антивирусных баз.

3.6. При необходимости разрабатывать инструкции по работе пользователей с программными средствами.

3.7. Проводить работы по обнаружению и обезвреживанию вирусов.

3.8. Участвовать в работе комиссии по расследованию причин заражения ПЭВМ и серверов.

3.9. Хранить эталонные копии антивирусных программных средств.

3.10. Осуществлять периодический контроль за соблюдением пользователями ПЭВМ требований настоящей Инструкции.

3.11. Разрабатывать инструкции по работе пользователей с системой антивирусной защиты информации.

3.12. Проводить периодический контроль работы программных средств системы антивирусной защиты информации на ПЭВМ (серверах).

Функции пользователей

Пользователи ИСПДн:

4.1. Получают по ЛВС или от Администратора безопасности ИСПДн носители с обновлениями антивирусных баз (в случае отсутствия механизмов централизованного распространения антивирусных баз).

4.2. Проводят обновления антивирусных баз на ПЭВМ (в случае отсутствия механизмов централизованного распространения антивирусных баз).

4.3. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) сотрудник самостоятельно или вместе с администратором безопасности ИСПДн должен провести внеочередной антивирусный контроль ПЭВМ. При необходимости он должен привлечь Администратора безопасности ИСПДн для определения факта наличия или отсутствия компьютерного вируса.

4.4. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов сотрудники обязаны:

− приостановить работу;

− немедленно поставить в известность о факте обнаружения зараженных вирусом файлов Администратора безопасности ИСПДн, а также остальных сотрудников, использующие эти файлы в работе;

− провести анализ необходимости дальнейшего использования зараженных вирусом файлов;

− провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта привлечь Администратора безопасности ИСПДн);

− в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, передать зараженный вирусом файл на съемном носителе Администратору безопасности ИСПДн для дальнейшей передачи его в организацию, с которой заключен договор на антивирусную поддержку;

− по факту обнаружения зараженных вирусом файлов составить служебную записку Администратору безопасности ИСПДн, в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации и выполненные антивирусные мероприятия.

Порядок пересмотр инструкции

5.1. Инструкция подлежит полному пересмотру в случае приобретения МБОУ «СОШ №32 с углубленным изучением отдельных предметов» новых средств защиты, существенно изменяющих порядок работы с ними.

5.2. В остальных случаях Инструкция подлежит частичному пересмотру.

5.3. Полный пересмотр данной Инструкции проводится с целью проверки соответствия

определенных данным документом мер защиты реальным условиям применения их в ИСПДн

- Учет и мониторинг граждан, находящихся в социально – опасном положении ;
- Электронное образование в Республике Татарстан;
- Барс – Бюджет

5.4. Изменения в Инструкции (сведения о них) фиксируется в листе регистрации изменений (Приложение 1).

5.5. Вносимые изменения не должны противоречить другим положениям Инструкции. При получении изменений к данной Инструкции, сотрудники организации в течение трех рабочих дней вносят свои предложения и/или замечания к поступившим изменениям

Ответственные за организацию и контроль выполнения инструкции

6.1. Ответственность за соблюдение требований настоящей Инструкции пользователями возлагается на всех сотрудников МБОУ «СОШ №32 с углубленным изучением отдельных предметов»

6.2. Ответственность за организацию контрольных и проверочных мероприятий по вопросам антивирусной защиты возлагается на Администратора безопасности ИСПДн.

6.3. Ответственность за общий контроль информационной безопасности возлагается на ответственного за обеспечение безопасности ПДн Баринова Е.Г.

ПРИЛОЖЕНИЕ 4
ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

ЛИСТ № _____ регистрации изменений в Инструкции

№ п/п	Дата	Внесенное изменение	Основание (наименование, № и дата документа)	Кем внесено изменение (должность, подпись)

ПРИЛОЖЕНИЕ 5

Лист ознакомления
с «Инструкцией по организации антивирусной защиты информационных систем персональных данных Муниципального бюджетного образовательного учреждения «Средняя общеобразовательная школа №32 с углубленным изучением отдельных предметов»

№ п/п	Фамилия И.О. сотрудника	Дата ознакомления	Расписка сотрудника в ознакомлении