МУНИЦИПАЛЬНОЕ АВТОНОМНОЕ
ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«СРЕДНЯЯ ШКОЛА № 42»
Петропавловска – Камчатского городского округа

683002, г. Петропавловск-Камчатский, ул. Савченко, 12, тел.: 8 (4152) 49-89-54; 8 (4152) 49-83-91
e-mail: school42_pkgo_42@mail.ru

УТВЕРЖДАЮ
Директор МАОУ «СШ №42»
Л.В. Артеменко
_____
«_____»_____201 г.

УТВЕРЖДЕНО

Приказом по МАОУ «СШ №42»
от _____ № _____

ПЛАН ЗАЩИТЫ

ИНФОРМАЦИОННЫХ РЕСУРСОВ МАОУ «СШ № 42» ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ И НЕЗАКОННОГО ВМЕШАТЕЛЬСТВА В ПРОЦЕСС ЕЕ ФУНКЦИОНИРОВАНИЯ

Для служебного пользования

Экз. № 3

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий документ разработан в соответствии с Постановлением Правительства РФ от 2 августа 2019 г. № 1006 «Об утверждении требований к антитеррористической защищенности объектов (территорий) Министерства просвещения Российской Федерации и объектов (территорий), относящихся к сфере деятельности Министерства просвещения Российской Федерации, и формы паспорта безопасности этих объектов (территорий), основе Концепции информационной безопасности МАОУ « и определяет комплекс организационно-технических мер по защите информационных ресурсов МАОУ «СШ № 42» (в дальнейшем ИС) от несанкционированного доступа (НСД) к циркулирующей в ней информации, а также незаконного вмешательства в процесс ее функционирования.

1.2. Документ не регламентирует вопросы охраны помещений и обеспечения сохранности и физической целостности компонентов ИС, защиты от стихийных бедствий (пожаров, наводнений), сбоев и отказов технических средств, сбоев в системе энергоснабжения и вопросы восстановления данных, а также меры обеспечения личной безопасности персонала.

1.3. Требования настоящего документа распространяются на все структурные подразделения МАОУ «СШ № 42», в которых осуществляется автоматизированная обработка подлежащей защите информации, а также подразделения, осуществляющие сопровождение, обслуживание и обеспечение нормального функционирования ИС МАОУ «СШ № 42».

2. ЦЕЛЬ И ЗАДАЧИ ЗАЩИТЫ

2.1. Основной целью, на достижение которой направлены все положения данного документа, является защита МАОУ «СШ № 42», ее клиентов и корреспондентов от возможного нанесения им ощутимого материального, морального или другого ущерба посредством случайного или преднамеренного несанкционированного вмешательства в процесс функционирования ИС МАОУ «СШ № 42» или несанкционированного доступа к циркулирующей в ней информации и ее незаконного использования.

2.2. Указанная цель достигается посредством обеспечения и постоянного поддержания следующих свойств информации и автоматизированной системы ее обработки:

- доступности обрабатываемой информации (устойчивого функционирования ИС, при котором пользователи системы имеют возможность получения необходимой им информации и результатов решения задач за приемлемое время);
- конфиденциальности определенной части информации, хранимой, обрабатываемой и передаваемой по каналам связи;
- целостности информации, хранимой и обрабатываемой в ИС и передаваемой по каналам связи.

2.3. Для достижения основной цели защиты и обеспечения указанных свойств ИС и циркулирующей в ней информации система безопасности ИС должна обеспечивать эффективное решение следующих задач:

- защиту ИС от вмешательства в процесс ее функционирования посторонних лиц (возможность использования автоматизированной подсистемы и доступ к ее ресурсам должны иметь только зарегистрированные установленным порядком пользователи - сотрудники структурных подразделений МОАУ «СШ № 42);
- разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам ИС (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям ИС для выполнения своих служебных обязанностей);
- регистрацию действий пользователей при работе с защищаемыми ресурсами ИС в системных журналах и периодический контроль корректности (правомерности) действий пользователей системы путем анализа содержимого этих журналов специалистами службы безопасности и/или администраторами информационной безопасности технологических участков;
- защиту хранимых и передаваемых по каналам связи данных от несанкционированной модификации (искажения), фальсификации, уничтожения и подтверждение аутентичности (авторства) электронных документов;
- защиту информации ограниченного распространения, хранимой, обрабатываемой и передаваемой по каналам связи, от несанкционированного разглашения (утечки);
- защиту от несанкционированной модификации (подмены, уничтожения) и контроль целостности используемых в ИС программных средств, а также

защиту системы от внедрения несанкционированных программ, включая компьютерные вирусы;

- контроль целостности операционной среды исполнения прикладных программ (решения прикладных задач) и ее восстановление в случае нарушения;

3. МЕРЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Поставленная основная цель защиты и решение перечисленных задач достигается:

- строгой регламентацией процессов обработки данных с применением средств автоматизации и действий сотрудников МАОУ «СШ № 42», использующих ИС, а также действий персонала, осуществляющего обслуживание и модификацию программных и технических средств ИС, на основе утвержденных руководством МАОУ «СШ № 42» организационно-распорядительных документов по вопросам обеспечения информационной безопасности;
- полнотой охвата всех аспектов проблемы, непротиворечивостью (согласованностью) и реальной выполнимостью требований организационно-распорядительных документов по вопросам обеспечения информационной безопасности в ИС;
- назначением и подготовкой должностных лиц (сотрудников), ответственных за организацию и осуществление практических мероприятий по обеспечению безопасности информации и процессов ее обработки;
- наделением каждого сотрудника МАОУ «СШ № 42» (пользователя) минимально необходимыми для выполнения им своих функциональных обязанностей полномочиями по доступу к ресурсам ИС;
- четким знанием и строгим соблюдением всеми сотрудниками, использующими и обслуживающими аппаратные и программные средства ИС, установленных требований по вопросам обеспечения безопасности информации;
- персональной ответственностью каждого сотрудника, участвующего в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющего доступ к ресурсам ИС за свои действия;
- строгим учетом всех подлежащих защите ресурсов системы (информации, задач, каналов, рабочих станций, серверов и т.д.);

- принятием эффективных мер обеспечения физической целостности технических средств и непрерывным поддержанием необходимого уровня защищенности компонентов ИС;
- применением физических и технических (программно-аппаратных) средств защиты ресурсов системы и непрерывной административной поддержкой их использования;
- проведением работы с персоналом (подбор, разъяснение, обучение и т.п.) и эффективным контролем за соблюдением сотрудниками МАОУ «СШ № 42» - пользователями ИС требований по обеспечению информационной безопасности;
- юридической защитой интересов МАОУ «СШ № 42» при взаимодействии подразделений МАОУ «СШ № 42» с внешними организациями (связанном с обменом информацией) от противоправных действий, как со стороны этих организаций, так и от несанкционированных действий обслуживающего персонала и третьих лиц;
- проведением постоянного анализа эффективности и достаточности принятых мер и применяемых средств защиты информации, разработкой и реализацией предложений по совершенствованию системы защиты ИС.

4. ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АС (ОСНОВНЫЕ ПОЛОЖЕНИЯ ПОЛИТИКИ БЕЗОПАСНОСТИ)

4.1. Организационные, технологические и технические мероприятия по защите информации в ИС МАОУ «СШ № 42» должны проводиться в соответствии с требованиям действующего законодательства - Постановлением Правительства РФ от 2 августа 2019 г. № 1006 «Об утверждении требований к антитеррористической защищенности объектов (территорий) Министерства просвещения Российской Федерации и объектов (территорий), относящихся к сфере деятельности Министерства просвещения Российской Федерации, и формы паспорта безопасности этих объектов (территорий), нормативных и иных документов Государственной технической комиссии при Президенте Российской Федерации (Гостехкомиссии России), Федерального агентства правительственной связи и информации при Президенте Российской Федерации (ФАПСИ), а также нормативно - методическими материалами и организационно - распорядительными документами МАОУ «СШ № 42» по вопросам обеспечения информационной безопасности в автоматизированных системах.

4.2. Все ресурсы ИС должны быть установленным порядком категорированы (для каждого ресурса должен быть определен требуемый уровень защищенности). Подлежащие защите ресурсы системы (информация, задачи, программы, рабочие станции, сервера и т.д.) подлежат строгому учету (на основе использования соответствующих формуляров или специализированных баз данных).

4.3. На всех рабочих системах (РС) ИС, подлежащих защите, должны быть установлены необходимые технические средства защиты (соответствующие требуемому уровню защищенности - категории РС). Для пользователей защищенных РМ (то есть РС, на которых обрабатывается защищаемая информация или решаются подлежащие защите задачи) должны быть разработаны необходимые технологические инструкции, включающие требования по обеспечению информационной безопасности. Эксплуатация в структурных подразделениях МАОУ «СШ № 42» защищенных РС должна быть разрешена только при наличии формуляров РС (паспортов-предписаний на их эксплуатацию, свидетельствующих о выполнении всех необходимых требований информационной безопасности).

4.4. Все сотрудники МАОУ «СШ № 42», использующие при работе ИС, должны быть ознакомлены с Планом защиты ИС в части, их касающейся, должны знать и неукоснительно выполнять технологические инструкции и “Общие обязанности сотрудников МАОУ «СШ № 42» по обеспечению безопасности информации при использовании ИС”. Доведение требований до лиц, допущенных к обработке защищаемой информации, должно осуществляться начальниками подразделений под роспись.

Сотрудники МАОУ «СШ № 42», допущенные к работе с ИС, должны нести персональную ответственность за нарушение установленного порядка автоматизированной обработки информации, правил хранения, использования и передачи находящихся в их распоряжении защищаемых ресурсов системы. Каждый сотрудник (при приеме на работу или при допуске к работе с защищаемыми ресурсами ИС) должен подписывать Соглашение-обязательство о соблюдении и ответственности за нарушение установленных требований по сохранению банковской, служебной и коммерческой тайны, а также правил работы с защищаемой информацией в ИС. Любое грубое нарушение порядка и правил работы в ИС сотрудниками МАОУ «СШ № 42» должно расследоваться. К виновным должны применяться адекватные меры воздействия. Мера ответственности персонала за действия, совершенные в нарушение установленных правил обеспечения безопасной автоматизированной обработки информации, определяется

нанесенным ущербом, наличием злого умысла и другими факторами по усмотрению руководства МАОУ «СШ № 42».

4.5. Допуск сотрудников МАОУ «СШ № 42» к работе с автоматизированной подсистемой и доступ к ее ресурсам должен быть строго регламентирован. Любые изменения состава и полномочий пользователей ИС должны производиться установленным порядком согласно “Инструкции по внесению изменений в списки пользователей ИС и наделению их полномочиями доступа к ресурсам системы”. Каждому сотруднику МАОУ «СШ № 42» (пользователю) должны предоставляться минимально необходимые для выполнения им своих функциональных обязанностей права и полномочия по доступу к ресурсам ИС (производственная необходимость предоставления сотрудникам полномочий и прав доступа к ресурсам ИС определяется руководством соответствующих структурных подразделений). Ни один сотрудник МАОУ «СШ № 42» не должен обладать всей полнотой полномочий для единоличного бесконтрольного уничтожения, изменения либо создания и авторизации ресурсов в ИС. Руководители структурных подразделений обязаны своевременно предоставлять заявки на предоставление своим сотрудникам или лишение (в случае увольнения, перевода, болезни и т.п.) сотрудников соответствующих прав доступа и полномочий по работе с ресурсами ИС.

4.6. Аппаратно-программная конфигурация рабочих мест (автоматизированных рабочих мест), на которых обрабатывается защищаемая информация (с которых возможен доступ к защищаемым ресурсам), должна соответствовать кругу возложенных на пользователей данной РС функциональных обязанностей. Все неиспользуемые в работе (лишние) устройства ввода-вывода информации (COM, LPT порты, дисководы НГМД, CD с других носителей информации) на таких РС должны быть отключены (удалены физически или логически), не нужные для работы программные средства и данные с дисков РС должны быть удалены.

Для упрощения сопровождения, обслуживания и организации защиты РС должны оснащаться программными средствами и конфигурироваться унифицировано (в соответствии с установленными правилами).

4.7. Ввод в эксплуатацию новых РС и все изменения в конфигурации технических и программных средств существующих РС в ИС должны осуществляться только установленным порядком согласно “Инструкции по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств РС ИС”.

4.8. Все программное обеспечение (разработанное специалистами УИ, полученное централизованно или приобретенной у фирм производителей) должно установленным порядком проходить проверку (испытания) в Управлении информатизации (УИ) и передаваться в фонд алгоритмов и программ (ФАП) или архив эталонных программ УИ. В АС должны устанавливаться и использоваться только полученные установленным порядком из ФАП программные средства. Использование в ИС ПО, не учтенного в ФАП (не зарегистрированного и не имеющего разрешения на использование в АС), запрещено.

4.9. Физическая целостность аппаратных компонентов защищенных РС должна обеспечиваться организационными мерами и применением механических запоров (при наличии), пломб (наклеек, печатей или т.п.) на блоках и устройствах средств вычислительной техники. Повседневный контроль за целостностью и соответствием печатей (пломб, наклеек) на системных блоках ПЭВМ должен осуществляться пользователями РС (АРМ) и администраторами информационной безопасности подразделений. Периодический контроль – руководителями подразделений и сотрудниками службы информационной безопасности.

4.10. Эксплуатация подлежащих защите РС должна осуществляться в помещениях, оборудованных автоматическими замками, средствами сигнализации и постоянно находящимися под охраной или наблюдением, исключающим возможность бесконтрольного проникновения в помещения посторонних лиц и обеспечивающим физическую сохранность находящихся в помещении защищаемых ресурсов (РС, документов, реквизитов доступа и т.п.). Размещение и установка технических средств ПЭВМ таких РС (АРМ) должна исключать возможность визуального просмотра вводимой (выводимой) информации лицами, не имеющими к ней отношения.

Уборка помещений с установленными в них ПЭВМ должна производиться в присутствии ответственного, за которым закреплены данные технические средства, или дежурного по подразделению с соблюдением мер, исключающих доступ посторонних лиц к защищаемым ресурсам.

В помещениях во время обработки и отображения на ПЭВМ конфиденциальной информации должны присутствовать только лица, допущенные к работе с данной информацией. Организация приема посетителей должна исключать возможность их визуального ознакомления с защищаемой информацией, к которой они не допущены.

4.11. Разработка ПО задач (комплексов задач), проведение испытаний разработанного и приобретенного ПО, передача ПО в эксплуатацию должна осуществляться в соответствии с утвержденным «Порядком разработки, проведения испытаний и передачи задач (комплексов задач) в эксплуатацию».

5. ПОРЯДОК ПЕРЕСМОТРА ПЛАНА ЗАЩИТЫ

5.1. План защиты подлежит ***частичному*** пересмотру в следующих случаях:

- при изменении конфигурации, добавлении или удалении программных и технических средств в ИС, не изменяющих технологию обработки информации;
- при изменении конфигурации и настроек технических средств защиты, используемых в ИС;
- при изменении состава и обязанностей должностных лиц - пользователей и обслуживающего персонала ИС и сотрудников, отвечающих за информационную безопасность в автоматизированной системе.

5.2. ***Профилактический*** пересмотр Плана защиты производится не реже 1 раза в год и имеет целью проверку соответствия определенных данным планом мер реальным условиям применения АПС и текущим требованиям к ее защите.

5.3. План защиты подлежит ***полному*** пересмотру в случае изменения технологии обработки информации или использовании новых технических средств защиты.

5.4. В случае частичного пересмотра могут быть добавлены, удалены или изменены различные приложения к Плану защиты ИС с обязательным указанием в листе регистрации изменений данных о том, кто, когда, с какой целью, какие изменения внес и кто санкционировал эти изменения.

5.5. Изменения, вносимые в план, не должны противоречить другим положениям Плана защиты и должны быть проверены на корректность, полноту и реальную выполнимость.

5.6. Любой пересмотр Плана защиты должен осуществляться с обязательным участием Администрации МАОУ «СШ № 42».

6. ОТВЕТСТВЕННЫЕ ЗА РЕАЛИЗАЦИЮ ПЛАНА ЗАЩИТЫ

6.1. Ответственность за реализацию и соблюдение требований данного документа сотрудниками, допущенными к работе с ИС, возлагается на начальников

структурных подразделений и системного администратора (ответственных за информационную безопасность в подразделениях и на технологических участках).

6.2. За реализацию положений Плана защиты, связанных с применением и администрированием технических средств защиты информации от НСД отвечает заместитель директора по ИОП.

6.3. Реализация положений Плана защиты, связанных с сопровождением программного обеспечения и обслуживания технических средств, возлагается на инженера-программиста.

6.4. Методическое руководство и контроль за выполнением требований настоящего документа возлагается на службу обеспечения информационной безопасности (ИОП).

7. ОСНОВНЫЕ ПОНЯТИЯ И ОПРЕДЕЛЕНИЯ

Под ***информационной системой*** (ИС) понимается организационно-техническая система, представляющая собой совокупность следующих взаимосвязанных компонентов:

- технических средств обработки и передачи данных (средств вычислительной техники и связи);
- методов и алгоритмов обработки данных в виде соответствующего программного обеспечения;
- информации (массивов, наборов, баз данных) на различных носителях;
- персонала,

объединенных по организационно-структурному, тематическому, технологическому или другим признакам для выполнения автоматизированной обработки информации (данных) с целью удовлетворения информационных потребностей государственных органов, государственных, общественных или коммерческих организаций и предприятий (юридических лиц), отдельных граждан (физических лиц) и иных участников процесса информационного взаимодействия.

Безопасность информации - такое состояние информации (информационных ресурсов) и автоматизированной системы ее обработки, при котором с требуемой надежностью обеспечивается защита информации (данных, ключей шифрования и т.д.) от утечки, хищения, утраты, несанкционированного уничтожения, модификации (подделки), несанкционированного копирования, блокирования и т.п.

Для защиты информации в любой ИС требуется создание специальной ***системы безопасности (системы защиты)***, представляющей собой совокупность специального персонала, организационных мер и мероприятий, а также физических и технических средств защиты, применяемых в соответствии с общим замыслом.

Набор правил, регламентирующих функционирование ИС в соответствии с необходимыми условиями обеспечения информационной безопасности, а так же действий персонала ИС в случае нарушения этих условий, называется ***политикой безопасности.***

План защиты - документ, содержащий общее описание политики безопасности ИС. План защиты предназначен для фиксирования на определенный момент времени состояния ИС (технологии обработки информации, списка пользователей - должностных лиц, перечня и настроек программных и аппаратных средств), выявленных значимых угроз безопасности ИС, установленных прав доступа пользователей к ресурсам ИС и конкретных мер и мероприятий по противодействию выявленным значимым угрозам.

ЛИСТ

регистрации изменений

Дата	Содержание вносимых изменений	Кем санкционировано изменение	Подпись лица, произведшего изменения

Приложение 1

Описание технологического процесса обработки данных в ИС

(Далее должно следовать конкретное описание подсистемы ИС (как объектов защиты) и используемых в них информационных технологий)

Примерный план описания:

- Назначение защищаемого объекта, его основные функции;
- Структура, состав и размещение основных элементов, информационные связи с другими объектами. Основные особенности защищаемого объекта;
- Используемые технологии (режимы) обработки и передачи информации, механизмы взаимодействия основных элементов (подсистем) защищаемого объекта;
- Категории информационных ресурсов подлежащие защите;
- Виды обрабатываемой информации;
- Категории пользователей и обслуживающего персонала, уровень их доступа к информации;
- Схемы потоков данных на всех технологических участках автоматизированной обработки информации в ИС.

Приложение 2

к Плану защиты

ОСНОВНЫЕ УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АС

(пути их реализации и способы нейтрализации)

На основе Концепции информационной безопасности ОРГАНИЗАЦИИ определяются наиболее опасные угрозы информационной безопасности, пути их реализации и способы нейтрализации характерные для конкретной автоматизированной системы при ее функционировании.

Пример

Угрозы системе электронного документооборота

(при автоматизированной обработке)

Угроза	Атака	Время проведения атаки	Объект атаки (местоположение атакуемого)	Субъект атаки (местоположение атаку.щего)	Код угрозы
Модификация электронных документов (ЭД)	Изменение ПО	Вне процесса функционирования системы	Любая станция ЛВС	Эта же станция ЛВС	И1
				Любая станция ЛВС → Сервер (через LOGIN SCRIPT)	
			Почтовый сервер	Почтовый сервер	
				Любая станция ЛВС	
			Сервер	С любой станции ЛВС	
	Неправильный ввод ЭД	В процессе функционирования системы	Любая станция ЛВС	Эта же станция ЛВС	И2
				Любая станция ЛВС → Сервер (через LOGIN SCRIPT)	

	Внедрение программной закладки	В процессе функционирования системы	Любая станция ЛВС	Эта же станция ЛВС	И3
				Любая станция ЛВС → Сервер (через LOGIN SCRIPT)	
			Почтовый сервер	Почтовый сервер	
				Любая станция ЛВС	
			Сервер	Любая станция ЛВС	
	Перехват ЭД	В процессе функционирования системы	Сервер	Любая станция ЛВС	И4
		В процессе передачи данных	Сеть передачи данных	Промежуточные узлы	И5
			Модем	Промежуточные узлы	

Угроза	Атака	Время проведения атаки	Объект атаки (местоположение атакуемого)	Субъект атаки (местоположение атаку.щего)	Код угрозы
Ввод несуществующего ЭД	Изменение ПО	Вне процесса функционирования системы	Любая станция ЛВС	Эта же станция ЛВС	И1
				Любая станция ЛВС → Сервер (через LOGIN SCRIPT)	
			Почтовый сервер	Почтовый сервер	
				Любая станция ЛВС	
			Сервер	Любая станция ЛВС	
	Внедрение программной закладки	В процессе функционирования системы	Любая станция ЛВС	Эта же станция ЛВС	И3
				Любая станция ЛВС → Сервер (через LOGIN SCRIPT)	
			Почтовый сервер	Почтовый сервер	
				Любая станция ЛВС	
			Сервер	Любая станция ЛВС	
	«Ручной ввод»	В процессе функционирования системы	Сервер	Любая станция ЛВС	И6
			Почтовый сервер	Почтовый сервер	
				Любая станция ЛВС	
			ЛВС	Любая станции ЛВС	
		В процессе передачи данных	Сеть передачи данных	Промежуточные узлы	И7

			Модем	Промежуточные узлы	
Нарушение конфиденциальности ЭД	Изменение ПО	Аналогично предыдущему случаю			
	Внедрение программной закладки				
	Просмотр с экрана	В процессе функционирования системы	Любая станция ЛВС	Любая станция ЛВС	И8
			Почтовый сервер	Почтовый сервер	
	Перехват ЭД	В процессе функционирования системы	ЛВС	Любая станция ЛВС	И4
		В процессе передачи данных	Сеть передачи данных	Промежуточные узлы	И5
			Модем		
	Несанкционированное копирование	Вне процесса функционирования системы	Сервер	Любая станция ЛВС	И9

Угроза	Атака	Время проведения атаки	Объект атаки (местоположение атакуемого)	Субъект атаки (местоположение атаку.щего)	Код угрозы
Отказ от факта получения ЭД	Изменение ПО	В процессе функционирования системы	Любая станция ЛВС	Любая станция ЛВС	И3
			Почтовый сервер	Почтовый сервер	
		В процессе передачи данных	Внешняя организация	Внешняя организация	
Отказ от авторства ЭД	Аналогично предыдущему случаю				
Дублирование ЭД	Изменение ПО	Аналогично предыдущему случаю			
	Внедрение программной закладки				
	«Повтор в сети»	В/Вне процесса функционирования системы	Сервер	Любая станция сети	И12
			ЛВС	Любая станция сети	
			Сеть передачи данных	Промежуточные узлы	
			Модем		
Потеря или уничтожение ЭД	Перехват ЭД	В процессе функционирования системы	Сервер	Любая станция сети	И4
			ЛВС	Любая станция сети	
			Сеть передачи данных	Промежуточные узлы	
			Модем		

	Несанкционированное копирование	Вне процесса функционирования системы	Сервер	Любая станция ЛВС	И9
	Изменение ПО	Аналогично предыдущему случаю			
	Внедрение программной закладки				
НСД к АРМ системы электронного документооборота	НСД	В/Вне процесса функционирования системы	Любая станция ЛВС	Эта же станция ЛВС	И13
				Любая станция ЛВС → Сервер (через LOGIN SCRIPT)	
			Почтовый сервер	Почтовый сервер	
				Любая станция ЛВС	
			Сервер	Любая станция ЛВС	
			Любая станция ЛВС	Из внешней сети (Internet)	

Угроза	Атака	Время проведения атаки	Объект атаки (местоположение атакуемого)	Субъект атаки (местоположение атаку.щего)	Код угрозы
НСД к каналу передачи данным	НСД к каналу	В процессе функционирования системы	ЛВС	Любая станция сети	И14
		В процессе передачи данных	Сеть передачи данных	Промежуточный узел	И15
			Модем		
Нападение из внешней сети	Атака из внешней сети	В/Вне процесса функционирования системы	Сервер		И18
			Станция сети		
			Модем		
			Маршрутизатор		
Нарушение работоспособности процесса функционирования системы	Изменение ПО, изменение конфигурации аппаратных средств, внедрение программных закладок	В/Вне процесса функционирования системы	На всех технологических участках	На всех технологических участках	И17
Несанкционированное конфигурирование маршрутизаторов	Несанкционированное конфигурирование маршрутизаторов	В/Вне процесса функционирования системы	Маршрутизаторы	Любая станция сети передачи данных	И18

Меры защиты от реализации угроз

Код угрозы	Меры защиты		
	Организационные	Физические	Технические
И1	1. Инструкция по внесению изменений в конфигурации ПО 2. Инструкции пользователям 3. Задание ответственности за нарушение установленных правил 4. Инструкция по изменению полномочий пользователей	1. Разграничение доступа в помещения 2. Физическая защита помещений	1. Запрет загрузки АРМ с гибких магнитных дисков 2. Защита исполняемых файлов от изменения 3. Замкнутая среда разрешенных для запуска программ для каждого пользователя системы 4. Периодический контроль целостности исполняемых файлов и настроек программных средств 5. Использование ЭЦП 6. Регистрация событий
И2	1. Двойной контроль при вводе 2. Контроль прохождения документов 3. Инструкции пользователям 4. Задание ответственности за нарушение установленных правил	Нет	1. Двойной контроль при вводе (при помощи ПО) 2. Контроль прохождения документов (при помощи ПО) 3. Регистрация событий
И3	1. Инструкция по внесению изменений в конфигурации ПО 2. Инструкции пользователям 3. Задание ответственности за нарушение установленных правил	1. Разграничение доступа в помещения 2. Физическая защита помещений	1. Запрет загрузки АРМ с гибких магнитных дисков 2. Защита исполняемых и системных файлов от изменения 3. Замкнутая среда разрешенных для запуска программ для каждого пользователя системы 4. Периодический контроль целостности системы

			5. Регистрация событий 6. Использование средств обнаружения нападений
И4	1. Инструкция по внесению изменений в конфигурации ПО 2. Инструкции пользователям 3. Задание ответственности за нарушение установленных правил 4. Инструкция по изменению полномочий пользователей	1. Разграничение доступа в помещения 2. Физическая защита помещений	1. Ограничение доступа к серверу по номеру сетевой карты 2. Разрешение доступа к серверу только с защищенных рабочих станций 3. Запрет одновременного доступа к серверу пользователей с одинаковым именем 4. Преобразование информации 5. Защита консоли сервера 6. Регистрация событий 7. Использование средств обнаружения нападений

Код угрозы	Меры защиты		
	Организационные	Физические	Технические
И5	1. Договор с внешней организаций	1. За рамками полномочий ОРГАНИЗАЦИИ	1. Преобразование информации 2. Использование ЭЦП 3. Контроль времени
И6	1. Инструкция по изменению полномочий пользователей 2. Инструкции пользователям 3. Задание ответственности за нарушение установленных правил	1. Изоляция защищаемой системы от других систем ОРГАНИЗАЦИИ	1. Ограничение доступа к РС, серверу и т.п. 2. Разрешение доступа к серверу только с защищенных рабочих станций 3. Ограничение доступа к серверу по номеру сетевой карты 4. Запрет одновременного доступа к серверу пользователей с одинаковым именем 5. Регистрация событий 6. Использование средств обнаружения нападений
И7	1. Договор с внешней организаций	1. За рамками полномочий ОРГАНИЗАЦИИ	1. Использование ЭЦП 2. Преобразование информации 3. Квитирование 4. Контроль времени
И8	1. Инструкции пользователям 2. Задание ответственности за нарушение установленных правил	1. Разграничение доступа в помещения 2. Физическая защита	1. Хранитель экрана 2. Ограничение доступа к РС

		помещений	3. Разграничение доступа к РС
И9	1. Инструкции пользователям 2. Задание ответственности за нарушение установленных правил	1. Разграничение доступа в помещения 2. Физическая защита помещений	1. Ограничение доступа к серверу по номеру сетевой карты 2. Разрешение доступа к серверу только с защищенных рабочих станций 3. Запрет одновременного доступа к серверу пользователей с одинаковым именем 4. Преобразование информации 5. Защита консоли сервера 6. Регистрация событий 7. Использование средств обнаружения нападений
И10	1. Договор с внешней организаций 2. Ведение архивов ЭПД и ЭД	1. За рамками полномочий ОРГАНИЗАЦИИ	1. Регистрация событий 2. Использование ЭЦП

Код угрозы	Меры защиты		
	Организационные	Физические	Технические
И11	1. Инструкции пользователям 2. Задание ответственности за нарушение установленных правил	1. Изоляция защищаемой системы от других систем МАОУ «СШ № 42»	1. Ограничение доступа к РС 2. Разграничение доступа к РС 3. Регистрация событий 4. Использование средств обнаружения нападений
И12	1. Инструкции пользователям 2. Задание ответственности за нарушение установленных правил 3. Ведение архивов ЭПД и ЭД	1. Изоляция защищаемой системы от других систем МАОУ «СШ № 42»	1. Квитирование 2. ЭЦП 3. Контроль времени 4. Регистрация событий
И13	1. Инструкции пользователям 2. Задание ответственности за нарушение установленных правил 3. Инструкция по использованию СЗИ от НСД 4. Ограничение людей, имеющих право конфигурировать маршрутизаторы	1. Разграничение доступа в помещения 2. Физическая защита помещений 3. Изоляция защищаемой системы от других систем МАОУ «СШ « 42»	1. Ограничение доступа к РС, серверу 2. Разграничение доступа пользователей к РС, серверу 3. Регистрация событий 4. Хранитель экрана 5. Изменение стандартного имени администратора системы защиты 6. Разрешение работы в сети только одного администратора системы защиты или администратора сети 7. Владельцем всех исполняемых файлов в системе, а также критических настроек должен быть администратор

			системы защиты 8. Использование средств обнаружения нападений 9. Использование межсетевых экранов Использование антивирусных программ 10. Использование всех встроенных в марщрутизаторы средств защиты
И14	1. Инструкции пользователям 2. Задание ответственности за нарушение установленных правил	1. Защита кабельной системы	Нет
И15	1. За рамками полномочий ОРГАНИЗАЦИИ		

Код угрозы	Меры защиты		
	Организационные	Физические	Технические
И16	1. Инструкции пользователям 2. Задание ответственности за нарушение установленных правил	1. Разграничение доступа в помещения 2. Физическая защита помещений	1. Ограничение доступа к архиву ЭПД 2. Резервное копирование 3. Использование антивирусных программ
И17	Все меры	Все меры	Все меры
И18	1. Инструкция по использованию Internet 2. Договор с внешней организацией 3. Инструкции пользователям 4. Задание ответственности за нарушение установленных правил		1. Ограничение числа используемых модемов 2. Физическая изоляция РС для доступа в глобальные сети от АРМ системы ЭП и ЭД 3. Ограничение доступа к РС, имеющим модемы 4. Регистрация событий 5. Использование средств обнаружения нападений 6. Использование межсетевых экранов 7. Использование всех встроенных в марщрутизаторы средств защиты

Приложение 3

Проект

к Плану защиты

НЕФОРМАЛЬНАЯ МОДЕЛЬ НАРУШИТЕЛЯ

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

Система защиты ИС МАОУ «СШ № 42» должна строиться исходя из следующих предположений о следующих возможных типах нарушителей правил безопасности в системе:

1. ***"Неопытный (невнимательный) пользователь"*** - сотрудник МАОУ «СШ № 42», который может предпринимать попытки выполнения запрещенных операций, доступа к недоступным ему защищаемым ресурсам ИС, ввода некорректных данных и т.п. действия по ошибке, некомпетентности или халатности без злого умысла и использующий при этом только штатные (доступные ему) аппаратные и программные средства.

2. ***"Любитель"*** - сотрудник МАОУ «СШ № 42», пытающийся преодолеть систему защиты без корыстных целей, с целью самоутверждения (из «спортивного интереса»). Для преодоления системы защиты и совершения запрещенных действий он может использовать различные методы получения дополнительных полномочий доступа к ресурсам (имен, паролей и т.п. других пользователей), недостатки в построении системы защиты и доступные ему штатные (установленные на рабочей станции) программы (несанкционированные действия посредством превышения своих полномочий на использование разрешенных средств). Помимо этого он может пытаться использовать дополнительно нештатные инструментальные и технологические программные средства (отладчики, служебные утилиты), самостоятельно разработанные программы или стандартные дополнительные технические средства.

3. ***"Внешний нарушитель (злоумышленник)"*** - постороннее лицо или сотрудник МАОУ «СШ № 42», действующий целенаправленно из корыстных интересов или из любопытства и «спортивного интереса», возможно в сговоре с другими лицами. Он может использовать весь набор методов и средств взлома систем защиты, характерных для сетей общего пользования (сетей X.25 или сетей на основе IP-протокола), включая удаленное внедрение программных закладок и использование специальных инструментальных и технологических программ, используя имеющиеся слабости в системе защиты узлов сети ИС.

4. "Внутренний злоумышленник" - сотрудник МАОУ «СШ № 42», действующий целенаправленно из корыстных интересов или мести за нанесенную обиду, возможно в сговоре с лицами, не являющимися сотрудниками МАОУ «СШ № 42». Он может использовать весь набор

методов и средств взлома системы защиты, включая агентурные методы получения реквизитов доступа, пассивные средства (технические средства перехвата без модификации компонентов системы), методы и средства активного воздействия (модификация технических средств, подключение к каналам передачи данных, внедрение программных закладок и использование специальных инструментальных и технологических программ), а также комбинации воздействий как изнутри, так и извне - из сетей общего пользования.

Нарушителем может быть лицо из следующих категорий персонала МАОУ «СШ № 42»:

- зарегистрированные пользователи системы (сотрудники подразделений МАОУ «СШ № 42»);
- персонал, обслуживающий технические средства ИС (инженеры);
- технический персонал, обслуживающий здания (уборщицы, электрики, сантехники и другие сотрудники, имеющие доступ в здания и помещения, где расположены компоненты ИС);;
- руководители различных уровней.

Посторонние лица, которые могут быть нарушителями:

- подрядчики (представители организаций, граждане);
- посетители (приглашенные по какому-либо поводу) представители организаций (преступных организаций, иностранных спецслужб) или лица, действующие по их заданию;
- представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации (энерго-, водо-, теплоснабжения и т.п.);
- лица, случайно или умышленно проникшие в сети ИС МАОУ «СШ № 42» из внешних сетей телекоммуникации.

Принимаются следующие ограничения и предположения о характере действий возможных нарушителей:

- работа по подбору кадров и специальные мероприятия исключают возможность создания коалиций нарушителей, т.е. объединения (сговора) и целенаправленных действий по преодолению подсистемы защиты двух и более нарушителей - сотрудников МАОУ «СШ № 42»;
- нарушитель скрывает свои несанкционированные действия от других сотрудников;
- несанкционированные действия могут быть следствием ошибок пользователей, администраторов безопасности, эксплуатирующего и обслуживающего персонала, а также недостатков принятой технологии обработки, хранения и передачи информации.

Приложение 4

к Плану защиты

ПРИМЕНЯЕМЫЕ В АС ОРГАНИЗАЦИИ ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ

1. Целью применения технических (программно-аппаратных) средств защиты является практическая реализация установленных Планом защиты ИС МАОУ «СШ № 42» правил регламентации действий сотрудников МАОУ «СШ № 42», обеспечение устойчивого функционирования ИС и защиты критических ресурсов от недопустимых воздействий.

2. На технические средства защиты ИС возлагается решение следующих задач:

- защита информационной системы от вмешательства лиц, не допущенных к работе с ней;
- разграничение доступа законных пользователей системы и программ к информационным, программным и аппаратным ресурсам системы в строгом соответствии с утвержденными правилами и установленными полномочиями пользователей;
- обеспечение целостности критических ресурсов системы (в том числе самих средств защиты) и среды исполнения прикладных программ;
- защита ИС от внедрения вредоносных программ и вирусов;
- защита данных, передаваемых по каналам связи от раскрытия, искажения, подмены и фальсификации;
- регистрация, сбор, упорядоченное хранение и выдача сведений о событиях, происходящих в ИС и имеющих отношение к ее безопасности.

3. Успешное применение технических средств защиты предполагает, что выполнение перечисленных ниже требований обеспечено организационными мерами и используемыми физическими средствами защиты:

- физическая целостность всех компонент ИС обеспечена;
- каждый сотрудник (пользователь системы) имеет уникальное системное имя и минимально необходимые для выполнения им своих функциональных обязанностей полномочия по доступу к ресурсам системы;
- использование на рабочих станциях ИС ОРГАНИЗАЦИИ инструментальных и технологических программ, позволяющих предпринять попытки взлома или обхода средств защиты, ограничено и строго регламентировано;
- в защищенной системе нет программирующих пользователей. Разработка и отладка программ осуществляется за пределами защищенной системы;
- все изменения конфигурации технических и программных средств РС ИС производятся строго установленным порядком только на основании распоряжений руководства

структурных подразделений МАОУ «СШ № 42» и после проверки на предмет их соответствия Плану защиты ИС МАОУ «СШ № 42»;

- сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т.п.) располагается в местах, недоступных для посторонних (специальные помещениях, шкафах, и т.п.).
- специальной службой защиты информации осуществляется непрерывное управление и административная поддержка функционирования средств защиты в соответствии с Планом защиты ИС МАОУ «СШ № 42»;
- обеспечена полнота и непротиворечивость требований Плана защиты ИС МАОУ «СШ № 42»;.

5. Конфигурация технических (программно-аппаратных) средств защиты ИС

5.1. Разграничение доступа к ресурсам ИС осуществляется посредством применения:

- механизмов избирательного управления доступом, основанных на использовании атрибутных схем;
- механизмов полномочного управления доступом, основанных на использовании меток конфиденциальности ресурсов и уровней допуска пользователей;
- механизмов обеспечения замкнутой среды доверенного программного обеспечения (индивидуальных для каждого пользователя списков разрешенных для запуска программ),

поддерживаемых механизмами идентификации (распознавания) и аутентификации (подтверждения подлинности) пользователей при их входе в систему.

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

5.2. Реализация политики безопасности осуществляется:

- встроенными средствами защиты сетевой операционной системы Windows NT 4.0, _____;
- встроенными средствами защиты СУБД _____;
- дополнительными программными и аппаратными средствами защиты локальных ресурсов PC в среде MS DOS/Windows3.1X, Windows 95 с централизованным контролем и управлением "Secret Net";
- средствами криптографической защиты хранимых и передаваемых по каналам связи данных (_____);

- средствами контроля и регистрации событий (систем регистрации "Secret Net", Novell NetWare, _____).

Установленная на АРМ система “Secret Net” предназначена для защиты локальных ресурсов данных АРМ и регистрации действий пользователей при их работе как с локальными, так и с сетевыми ресурсами системы.

Система разграничения доступа сетевой ОС Novell NetWare v 4.11 (_____) - предназначена для защиты данных, хранимых на файловых серверах сети.

Гарантии корректности функционирования технических средств защиты обеспечиваются их производителями.

5.3. Встроенные средства защиты сетевой ОС обеспечивают на всех серверах и рабочих станциях:

- идентификацию по имени и аутентификацию пользователей по паролю при входе в сеть;
- авторизацию доступа к сетевым ресурсам;
- контроль доступа к удаленным дискам, каталогам и файлам на файловых серверах;
- группирование пользователей и контроль доступа к сетевым ресурсам на основе авторизации групповых полномочий и использования службы системного каталога (NDS);
- авторизацию привилегированных операций для пользователей, обладающих привилегиями;
- управление сетевой парольной защитой;
- защиту от перехвата сетевых паролей.

5.4. Средства защиты "Secret Net" обеспечивают на всех рабочих станциях:

- идентификацию по имени (по устройству индивидуальной идентификации Smart Card или Touch Memory при наличии аппаратной поддержки) и аутентификацию пользователей по паролю при входе в систему с рабочих станций;
- управление парольной защитой на рабочих станциях;
- авторизацию доступа к локальным ресурсам станций;
- контроль доступа типа “чтение”, “запись”, “исполнение” к локальным физическим и логическим дискам, к системным и пользовательским каталогам и файлам;
- группирование пользователей и разграничение доступа к локальным ресурсам на основе авторизации групповых полномочий;
- затирание остаточной информации на магнитных носителях при удалении файлов;
- защиту от перехвата паролей;
- аппаратно-программную защиту от несанкционированной загрузки ОС на рабочих станциях с гибких магнитных дисков;
- защиту от вирусного заражения РС путем контроля модификации программных файлов и системных областей дисков;
- защиту от внедрения посторонних (нелегальных) программ путем создания замкнутой среды доверенного программного обеспечения;
- резервное копирование (и автоматическое восстановление при искажении) системных областей дисков;
- оперативное оповещение администратора безопасности об активности рабочих станций сети и пользователей, а также обо всех происходящих на рабочих станциях попытках НСД.

5.5. Используемые средства регистрации

Средства объективного контроля обеспечивают обнаружение и регистрацию событий, которые могут повлечь за собой нарушение политики безопасности и привести к возникновению кризисных ситуаций.

Средства контроля и регистрации системы состоят из:

- системных средств;
- сетевых средств;
- дополнительных (прикладных) средств.

Системные средства контроля и регистрации системы "Secret Net" предоставляют возможности:

- ведения и анализа журналов регистрации событий безопасности (системных журналов). Журналы регистрации ведутся для каждой рабочей станции сети;
- оперативного ознакомления администратора с содержимым системного журнала любой станции и с журналом оперативных сообщений об НСД;
- получения твердой копии (печати) системного журнала (преобразования в текстовый файл или файл .DBF);
- упорядочения системных журналов по дням и месяцам, а также установления ограничений на срок их хранения;
- оперативного оповещения администратора о нарушениях безопасности.

При регистрации событий безопасности в системном журнале фиксируется следующая информация:

- дата и время события;
- идентификатор субъекта (пользователя, программы), осуществляющего регистрируемое действие;
- действие (если регистрируется запрос на доступ, то отмечается объект и тип доступа).

Средства контроля обеспечивают обнаружение и регистрацию более 90 типов событий, в том числе:

- вход пользователя в систему;
- вход пользователя в сеть;
- неудачная попытка входа в систему или сеть (неправильный ввод пароля);
- подключение к файловому серверу;
- запуск программы;
- завершение программы;
- оставление программы резидентно в памяти;
- попытка открытия файла недоступного для чтения;
- попытка открытия на запись файла недоступного для записи;
- попытка удаления файла недоступного для модификации;
- попытка изменения атрибутов файла недоступного для модификации;
- попытка запуска программы, недоступной для запуска;

- запрещенная групповая операция с файлами;
- попытка получения доступа к недоступному каталогу;
- попытка чтения/записи информации с диска, недоступного пользователю;
- попытка запуска программы с диска, недоступного пользователю;
- синхронизация времени и даты с файловым сервером;
- нарушение целостности программ и данных системы защиты
- и др.

Системные журналы всегда первоначально формируются на дисках рабочих станций. Перенос их на файловый сервер осуществляется автоматически при начальной загрузке рабочих станций и оперативно по требованию администратора.

5.6. Используемые средства криптографической защиты информации

Для защиты каких данных, передаваемых по каналам связи, используется электронная цифровая подпись (ЭЦП) и шифрование блоков передаваемой информации.

Центр генерации ключей шифрования и ЭЦП, их учета и распространения находится в (каком подразделении, кто отвечает). Генерация ключей осуществляется на специальных РС (АРМ). Территориально эти РС расположены в специально оборудованном помещении. Ключевая информация не хранится на жестких дисках РС.

6. Управление средствами защиты осуществляется с помощью:

- средств интерфейса администратора безопасности - для защиты локальных разделяемых наборов данных, наборов данных, содержащих конфиденциальную информацию, устройств и других защищаемых ресурсов рабочих станций;
- средств интерфейса администратора сети - для защиты сетевых наборов данных и устройств;
- средств интерфейса пользователя - для защиты личных наборов данных;
- дополнительных программных средств (для управления ключами и т.п.).

6.1. Средства управления администратора безопасности позволяют осуществлять:

- централизованное (с АРМ администратора безопасности) создание (регистрацию) и удаление пользователей всех защищенных Secret Net PC, изменение их полномочий и паролей;
- установку атрибутов доступа пользователей к локальным ресурсам;
- централизованное создание, удаление и изменение состава групп пользователей, а также их прав доступа;
- централизованное управление оперативным оповещением об НСД;

- централизованное управление регистрацией событий и анализ системных журналов;
- как локальное (непосредственно с рабочей станции), так и удаленное (с АРМ администратора) управление средствами защиты, установленными на рабочих станциях.

6.2. Средства управления администратора сети позволяют осуществлять:

- создание и удаление пользователей сети, изменение их полномочий по доступу к сетевым ресурсам и изменение их сетевых паролей;
- установку атрибутов доступа пользователей к сетевым ресурсам;
- создание, удаление и изменение состава групп сетевых пользователей, а также их прав доступа.

6.3. Средства управления пользователя позволяют осуществлять:

- изменение своего пароля входа в систему;
- установку на РС атрибутов доступа к локальным ресурсам, владельцем которых является данный пользователь.

Документация по средствам защиты и контроля (руководства пользователя, администратора, системного программиста) позволяет контролировать средства защиты на уровне пользователя или администратора безопасности.

7. Общие настройки применяемых технических средств защиты

7.1. Настройки сетевой ОС Novell NetWare

Для обеспечения эффективной защиты сетевых ресурсов ЛВС применяются следующие общие настройки средств разграничения доступа ОС Novell NetWare:

- для каждого сотрудника МАОУ «СШ № 42» заводится персональный сетевой счет (имя пользователя);
- устанавливается обязательное наличие у пользователя сетевого пароля;
- устанавливается режим принудительной смены пароля пользователем через определенный промежуток времени;
- устанавливается необходимость использования уникального пароля, а также пароля отличного от имени пользователя;
- производится привязка пользователя к конкретным компьютерам, с которых тот может работать в сети (по номеру сетевых плат);
- устанавливается ограничения по времени работы пользователя в сети;
- устанавливается режим контроля за доступом пользователя к ресурсам серверов сети.

Круг рабочих станций, с которых разрешен доступ к системе с правами суперпользователя (администратора сети), ограничен средствами Novell NetWare.

Настройки системы Secret Net (ПРИМЕР)

Общие настройки системы защиты Secret Net

Название параметра	Значение параметра
Мин. Количество символов в пароле	8
Работа в сети станций, не оснащенных системой защиты	Нет
Количество администраторов в системе	1
Время хранения системного журнала	не менее 90 дней

Группы пользователей, существующие в системе

Имя группы	Кто входит в эту группу
ADMGROUP	Администраторы системы
PERSONAL	Все пользователи системы
...	

Установки компьютера по умолчанию

Данные установки по умолчанию присваиваются каждой рабочей станции сети, на которой установлены средства защиты Secret Net.

Название параметра	Значение параметра
Имя пользователя по умолчанию	
Время ожидания ввода пароля	20 сек
Максимальный размер журнала	15 блоков (по 64 Кбайт)

Пользователи, создаваемые на каждой рабочей станции, при установке на нее системы защиты “Secret Net” и их атрибуты

Сведения о пользователях и их полномочиях переносятся на каждую рабочую станцию сети при установке на нее системы Secret Net.

Имя пользователя: SUPERVISOR

Наличие привилегии у пользователя	Название привилегии	
X	Запрос пароля	
	Список задач	
	Запрет COM1-COM4	
	Запрет INT 13/25/26	
X	Автоматический ввод пароля	
	Запрет доступа к принтеру	
	Затирание данных	
	Запрет изменения AUTOEXEC	
X	Вывод сообщения на экран	
	Печать системного журнала	
	Контроль целостности программ	
Уровень	Тип регистрации	
Регистрации	Минимальный	Максимальный

Наличие привилегии у пользователя	Название привилегии	
Сетевой	X	
Локальный	X	

Для перекрытия путей внедрения программных закладок на защищаемых РС должна создаваться и поддерживаться замкнутая среда доверенного контролируемого программного обеспечения, в которой:

- должна быть исключена возможность произвольного использования инструментальных программ, с помощью которых можно было бы осуществить корректировку данных и программ на носителях и в памяти;
- списки программ, с которыми каждый пользователь имеет право работать, должны содержать минимальный набор действительно необходимых для выполнения их функциональных обязанностей программ;
- в защищенной системе не должно быть программирующих пользователей, способных создать свои инструментальные средства взлома системы защиты (разработка и отладка программ должна производиться на компьютерах, не входящих в состав защищенной системы);
- все используемые программы должны проходить предварительную сертификацию на предмет отсутствия в них закладок (по возможности с анализом всех исходных текстов, документации и т.д.);
- все санкционированные доработки программ также должны проходить сертификацию на безопасность;
- целостность и неискаженность программ должна периодически проверяться путем проверки его характеристик (длины, контрольной суммы).

Ниже приводится определения и толкования названий и терминов, используемых в Приложениях и встречающихся в формулярах.

Название термина	Что означает
Системное имя пользователя	Имя пользователя, которое он должен ввести при входе в систему
Список групп, в которые входит пользователь	Список групп пользователей, в которые входит данный пользователь, что позволяет ему получить доступ к файлам (каталогам) в соответствии с правами, установленными для группы

Название привилегии	Что означает для пользователя, если в поле привилегии установлен символ «X»
Запрос пароля	При входе в систему у пользователя будет запрошен пароль
Список задач	Для пользователя установлен режим замкнутой программной среды
Запрет COM1-COM4	Пользователю запрещен вывод данных через коммуникационные порты
Запрет INT 13/25/26	Программам пользователя запрещено обращение к локальным жестким дискам напрямую
Автоматический ввод пароля	При входе пользователя в сеть Novell NetWare его пароль будет вводиться автоматически системой защиты
Запрет доступа к принтеру	Пользователю запрещен доступ к локальному принтеру
Затирание данных	При удалении файлов программами пользователя содержимое файлов затирается специальной последовательностью
Запрет изменения AUTOEXEC	Пользователю запрещено изменение файла AUTOEXEC.BAT
Вывод сообщения на экран	При возникновении событий НСД на экране появляется сообщение о запрете доступа
Печать системного журнала	Пользователю разрешена печать системного журнала на принтере
Контроль целостности программ	При загрузке системы защиты будет контролироваться целостность файлов, разрешенных для запуска пользователю
Тип регистрации / Локальный (Минимальный /максимальный)	Обеспечивает управление подробностью регистрации событий, связанных с обращением программ пользователя к локальным ресурсам
Атрибуты пользователя по умолчанию	Атрибуты управления доступом, устанавливаемые на создаваемые пользователем на локальных дисках каталоги и файлы
Доступ к дискам	Определяет тип доступа к локальным дискам, установленным на компьютере.
Название права	Что означает, если поле права доступа установлен символ «X»
Чтение (R)	Позволяет читать содержимое объекта (файла), позволяет запускать программы из каталога

Запись (W)	Позволяет записывать содержимое объекта (файла), позволяет удалять файл (каталог) и изменять атрибуты файла (каталога)
Исполнение (R)	Позволяет запускать программу
Название настройки	Назначение настройки
Имя пользователя по умолчанию	Имя пользователя, которое предлагается системой защиты при ее загрузке
Имя диска системного журнала	Имя диска, на котором хранится системный журнал
Время ожидания ввода имени	Время ожидания системой ввода имени пользователя. По истечении этого интервала система автоматически переходит к запросу пароля. При отсутствии пароля производится загрузка компьютера
Мягкий режим контроля для программ	Позволяет запускать программы, которые не входя в список разрешенных для запуска
Мягкий режим контроля для атрибутов	Позволяет программам пользователя работать с файлами (каталогами), частично недоступными по различным атрибутам управления доступа
Действия при изъятии карты идентификации	Определяет тип действий, предпринимаемых системой защиты при обнаружении изъятия карты идентификации
Действия при нарушении целостности системы защиты	Определяет тип действий, предпринимаемых системой защиты при обнаружении нарушения целостности системы защиты
Режимы работы/Полномочное управление	Управляет включением/отключением полномочного (мандатного) управления доступом
Режимы работы/Пароль в идентификаторе	Управляет хранением пароля пользователя в идентификаторе
Режимы работы/Регистрация событий управления	Управляет регистрацией событий по управлению доступом
Интервал паузы неактивности	Определяет длительность паузы неактивности пользователя, по истечении которой система защиты автоматически блокирует клавиатуру и экран
Количество циклов стирания	Определяет количество повторов затирания содержимого файлов при их удалении
Мин. количество символов в пароле	Минимальное количество символов в пароле

Работа в сети станций, не оснащенных системой защиты	Если в поле есть отметка - возможно подключение к основному файловому серверу пользователей с незащищенных рабочих станций
Количество администраторов в системе	Количество администраторов системы, которые могут одновременно работать в системе
Время хранения системного журнала	Количество дней, в течении которых необходимо хранение системного журнала