

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Политехнический институт
Факультет приборостроения,
информационных технологий и
электроники

Кафедра
«Информационная безопасность
систем и технологий»

Специальность 10.05.02 –

Информационная безопасность
телекоммуникационных систем

Специализация -

Разработка защищенных
телекоммуникационных систем

ДИПЛОМНЫЙ ПРОЕКТ

на тему

ПОДСИСТЕМА НАСТРОЙКИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ
ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Студент _____ Коробов Дмитрий
Андреевич

Руководитель _____ Лыдин С.С.

Нормоконтролёр _____ Фатеев А.Г.

Рецензент руководитель
информационно-аналитической группы _____ Рябов А.С.

Работа допущена к защите (протокол заседания кафедры от _____ № _____)

Заведующий кафедрой _____ С.Л. Зефилов

Работа защищена с отметкой _____ (протокол заседания ГЭК
от _____ № _____)

Пенза 2016

РЕФЕРАТ

Отчет содержит 168 с., 61 рис., 8 табл. , 12 источников, 1 прил.

СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ, НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП, ИНФОРМАЦИОННАЯ СИСТЕМА, ПОДСИСТЕМА НАСТРОЙКИ, ПРОБЛЕМЫ ПРОЕКТИРОВАНИЯ, ТРЕБОВАНИЯ К ПОДСИСТЕМЕ НАСТРОЙКИ, ПОЛЬЗОВАТЕЛЬСКИЙ ИНТЕРФЕЙС.

Целью дипломного проекта является разработка подсистемы настройки средств защиты информации от несанкционированного доступа, отвечающей требованиям полноты функционала и удобства использования.

Актуальность дипломного проекта состоит в том, что на данный момент не существует общепринятого подхода к проектированию средства защиты информации от несанкционированного доступа, который обеспечивал бы возможность выполнения эксплуатирующей организацией требований нормативных документов в области защиты информации без существенного снижения требуемого уровня защищенности вследствие некорректной настройки.

Объектами исследования дипломного проекта являются отечественные нормативно-методические документы по обеспечению информационной безопасности, а также подсистемы настроек существующих средств защиты информации от несанкционированного доступа.

Объектом разработки дипломного проекта является подсистема настройки средств защиты информации от несанкционированного доступа.

Необходимая цель достигается путем решения следующих задач: анализ факторов определяющих требование к подсистемам настройки средств защиты информации, исследование подсистем настройки в существующих средствах защиты информации, выявление сложностей, связанных с проектированием подсистем настройки средств защиты информации, анализ технических требований по обеспечению информационной безопасности информационных

систем, содержащихся в отечественных нормативно-методических документах, разработка требований к подсистеме настройки и проектирование подсистемы настройки средств защиты информации от несанкционированного доступа.

СОДЕРЖАНИЕ

Введение	9
1 Анализ факторов, определяющих требования к подсистемам настройки средств защиты информации	11
2 Исследование подсистем настройки в существующих на рынке средствах защиты информации.	15
2.1 Выбор технических решений.....	15
2.2 СЗИ от НСД «Страж NT» (версия 4.0)	15
2.3 Secret Net 7.....	28
2.4 Аккорд-Win 64 (TSE).....	43
2.5 Вывод	54
3 Постановка проблем проектирования подсистемы настройки средств защиты информации.	55
3.1 Особенности существующих на рынке средств защиты информации от несанкционированного доступа и их подсистем настройки.....	55
3.2 Проблемы администрирования средств защиты информации от несанкционированного доступа.....	56
3.3 Вывод.....	57
4 Анализ технических требований по обеспечению информационной безопасности информационных систем, содержащихся в отечественных нормативно-методических документах.....	59
4.1 Объекты исследования	59
4.2 Исследование требований к различным типам информационных систем.....	61
4.2.1 Идентификация и аутентификация.....	61

4.3 Управление доступом субъектов доступа к объектам доступа.....	62
4.3.1 Ограничение программной среды	64
4.3.2 Защита машинных носителей информации.....	64
4.3.3 Регистрация событий безопасности	65
4.3.4 Антивирусная защита.....	66
4.3.5 Обнаружение вторжений	66
4.3.6 Контроль (анализ) защищенности информации.....	66
4.3.7 Обеспечение целостности информационной системы и информации	67
4.3.8 Обеспечение доступности информации.....	68
4.3.9 Защита среды виртуализации.....	69
4.3.10 Защита технических средств	70
4.3.11 Защита информационной системы, ее средств, систем связи и передачи данных.....	71
4.3.12 Другие группы требований к ИС	75
4.4 Исследование требований к автоматизированным системам	75
4.5 Исследование требований к средствам вычислительной техники.....	77
4.6 Вывод.....	79
5 Классификация технических требований в зависимости от степени и характера влияния на компоненты подсистемы настройки средств защиты информации от несанкционированного доступа	80
5.1 Требования к средствам защиты информации от несанкционированного доступа.....	80

5.2	Высокоуровневые требования к подсистеме настройки средств защиты информации от несанкционированного доступа.....	82
5.3	Номенклатура компонентов подсистемы настройки средства защиты информации от несанкционированного доступа.....	84
5.4	Вывод.....	95
6	Формирование комплекса требований к подсистеме настройки средств защиты информации от несанкционированного доступа.....	96
6.1	Требования по защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах.....	96
6.2	Низкоуровневые требования к подсистеме настройки средств защиты информации от несанкционированного доступа.....	99
7	Проектирование подсистемы настройки средства защиты информации от несанкционированного доступа.....	107
7.1	Состав интерфейсов взаимодействия подсистемы настройки с внешними подсистемами.....	107
7.2	Требования к интерфейсу взаимодействия идентификации и аутентификации с подсистемой настройки.....	107
7.3	Требования к интерфейсу взаимодействия подсистемы управления доступом с подсистемой настройки.....	112
7.4	Требования к интерфейсу взаимодействия подсистемы замкнутой программной среды с подсистемой настройки.....	126
7.5	Требования к интерфейсу взаимодействия управления носителями информации с подсистемой настройки.....	128

7.6Требования к интерфейсу взаимодействия регистрации и учета с подсистемой настройки.....	130
7.7Требования к интерфейсу взаимодействия контроля целостности с подсистемой настройки.....	132
8 Проектирование типовых элементов пользовательского интерфейса подсистемы настройки средства защиты информации от несанкционированного доступа.....	149
8.1Методы повышения удобства пользовательского интерфейса подсистемы настройки средства защиты информации от несанкционированного доступа при использовании мировых практик .	149
8.2 Подсистема настройки идентификации и аутентификации.....	150
8.3Подсистема настройки управления доступом.....	153
8.4Подсистема настройки замкнутой программной среды.	159
8.5Подсистема настройки управления носителями информации	160
8.6Подсистема настройки регистрации и учета.....	161
8.7Подсистема настройки контроля целостности.....	162
Заключение	164
Список использованных источников	166
Приложение А Результаты прохождения проверки «Антиплагиат».....	168

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АПМДЗ – аппаратно-программный модуль доверенной загрузки

АРМ – автоматизированное рабочее место

АС – автоматизированная система

ЗИ – защита информации

ЗПС – замкнутая программная среда

ИС – информационная система

КС – контрольная сумма

КЦ – контроль целостности

НСД – несанкционированный доступ

ОС – операционная система

ПАК – программно-аппаратный комплекс

ПДн – персональные данные

ПО – программное обеспечение

ПРД – правила разграничения доступа

РФ – Российская Федерация

СВТ – средство вычислительной техники

СЗИ – средство защиты информации

СКЗИ – средство криптографической защиты информации

СОВ – средство обнаружения вторжений

ФСТЭК – федеральная служба по техническому и экспортному контролю.

ВВЕДЕНИЕ

Современный мир невозможно представить без ИС. Преимуществами ИС является повышение производительности и коммуникации организаций. Одной из важных проблем информационной безопасности ИС является несанкционированный доступ к информации. ФСТЭК устанавливает состав, и содержание технических мер по обеспечению безопасности данных при их обработке в информационных системах.

Существуют программные и программно-аппаратные комплексы, позволяющие информационной системе в полной мере удовлетворять требованиям ФСТЭК, в частности противодействовать несанкционированному доступу.

Немаловажную роль в СЗИ от НСД играет подсистема настройки средств защиты информации. Она позволяет конфигурировать различные компоненты средства защиты информации от несанкционированного доступа. Но проблемы, возникающие еще на стадии проектирования подсистемы настройки, могут повлиять на функциональность, а также снизить обеспечиваемый уровень безопасности информации.

Целью дипломного проекта является разработка подсистемы настройки средств защиты информации от несанкционированного доступа, отвечающей требованиям полноты функционала и удобства использования.

Необходимая цель достигается путем решения следующих задач: анализ факторов определяющих требование к подсистемам настройки средств защиты информации, исследование подсистем настройки в существующих средствах защиты информации, выявление сложностей, связанных с проектированием подсистем настройки средств защиты информации, анализ технических требований по обеспечению информационной безопасности информационных систем, содержащихся в отечественных нормативно-методических документах,

разработка требований к подсистеме настройки и проектирование подсистемы настройки СЗИ от НСД.

.

1 Анализ факторов, определяющих требования к подсистемам настройки средств защиты информации

В настоящее время эксплуатируются различные системы, в которых производится обработка информации ограниченного доступа: государственные информационные системы, информационные системы персональных данных и другие, автоматизированные системы управления технологическими процессами и др.

Штатные механизмы защиты операционных систем, используемых в ИС, не в полной мере удовлетворяют требованиям ФСТЭК. Поэтому применяются внешние сертифицированные средства защиты информации.

Одной из важных проблем информационной безопасности является несанкционированный доступ к информации. Построение комплекса ЗИ от НСД в каждой конкретной ИС начинается с изучения информационных потоков в ИС, определяются риски и основные угрозы информации на всех этапах ее хранения, обработки и передачи в ИС. На основании полученной информации строится матрица доступа к информации, обрабатываемой в информационной системе, а также схема информационных потоков. Затем на основании собранных об ИС сведений строится модель комплекса СЗИ от НСД для исследуемой ИС.

В настоящее время в ИС для обеспечения ЗИ от НСД применяются следующие классы средств защиты:

- средства аппаратной идентификации;
- средства антивирусной защиты;
- средства обнаружения вторжений;
- межсетевые экраны;
- программные и программно-аппаратные средства защиты информации от несанкционированного доступа (СЗИ от НСД);
- средства шифрования и др. [1].

Основную роль в обеспечении безопасности в информационной системе играют СЗИ от НСД. В данный момент на рынке средств защиты предлагается обширный выбор СЗИ от НСД, основными из которых являются «Аккорд», «Страж» и Secret Net. Данные программные и программно-аппаратные комплексы обеспечивают безопасность информационной системы в соответствии с требованиями ФСТЭК.

Если рассматривать средство защиты информации от несанкционированного доступа как систему, то можно выделить в ней несколько подсистем. Одной из таких подсистем является подсистема настройки СЗИ от НСД. Она необходима для конфигурирования других компонентов средства защиты информации от несанкционированного доступа.

Согласно руководящему документу «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» СЗИ от НСД должно обеспечивать безопасность информации с помощью следующих четырех основных подсистем:

- идентификации и аутентификации;
- регистрации и учета;
- криптографической защиты;
- контроля целостности [1].

Подсистема идентификации и аутентификации предоставляет и контролирует доступ к работе на АРМ АС пользователей. В зависимости от особенностей ИС, на которой эта информация обрабатывается, могут применяться разные методы идентификации и аутентификации. Однако стоит отметить, что усиленным методом является аппаратная идентификация с последующей аутентификацией по паролю определенной длины и сложностью.

К основным задачам подсистемы регистрации и учета относятся:

- ведение журнала всех действий пользователя;

- фиксация в журнале попыток НСД пользователя к ресурсам, доступ к которым ему запрещен;
- учет всех носителей информации и гарантированное уничтожение затираемой информации [1].

Для учета носителей в СЗИ применяются «белые» списки носителей по их серийным номерам, определяемым при подключении к АРМ, и список атрибутов по доступу к ним. Это позволяет избежать несанкционированного копирования информации и, как результат, утечки ее с использованием сторонних носителей. Кроме того, удастся избежать заражения АРМ АС вирусами. Однако при настройке данной подсистемы необходимо тщательно изучить процесс работы пользователей АС, так как жесткая настройка без учета тонкостей циркуляции информации может привести к значительному ухудшению удобства применения СЗИ от НСД конечными пользователями и, как результат, к новым попыткам НСД.

Подсистема криптографической защиты преобразовывает информацию, обрабатываемую в АС, с помощью криптографических алгоритмов. Чаще всего информация зашифровывается при передаче по сети, реже — при ее сохранении на съемные носители [1].

Основной задачей подсистемы контроля целостности является сохранение работоспособности как программной, так и аппаратной части АС. В обязанности СЗИ от НСД входят подсчет контрольных сумм программного обеспечения АС и контроль аппаратной конфигурации АС. В случае несовпадения контрольных сумм и (или) изменения аппаратной конфигурации компьютера работа текущего пользователя блокируется. Контроль проводится в два этапа:

- по завершении работы пользователя СЗИ от НСД вычисляет контрольные суммы программ и сохраняет аппаратную конфигурацию АС;

– при следующем включении АРМ АС на этапе загрузки операционной системы и СЗИ от НСД контрольные суммы и аппаратная конфигурация сравниваются с эталонными значениями. По результатам сравнения принимается решение о возможности дальнейшей работы пользователя на АС [1].

Из вышесказанного можно сделать следующий вывод: настройка СЗИ от НСД зависит от многих факторов, а именно желание заказчика, особенности конкретной ИС, требования к обеспечению безопасности и другие. Учет всех тонкостей работы с информацией в ИС, а также анализ угроз безопасности информации и соблюдение требований руководящих документов обеспечивают СЗИ от НСД в ИС и, что немаловажно, удобную, комфортную работу пользователей.

2 Исследование подсистем настройки в существующих на рынке средствах защиты информации.

2.1 Выбор технических решений

Для определения типовых подсистем настройки, необходимо на примере разобрать несколько существующих на рынке СЗИ от НСД. В работе рассматриваются сертифицированные, а также наиболее распространенные на рынке СЗИ от НСД такие как: «Страж NT» (версия 4.0), Secret Net 7 и ПАК «Аккорд-Win64».

2.2 СЗИ от НСД «Страж NT» (версия 4.0)

Система защиты информации от несанкционированного доступа «Страж NT» (версия 4.0) представляет собой программный комплекс средств защиты информации с использованием аппаратных идентификаторов. СЗИ от НСД «Страж NT» (версия 4.0) предназначена для комплексной защиты информационных ресурсов от несанкционированного доступа и функционирует в среде 32-х и 64-разрядных операционных систем Microsoft Windows.

СЗИ от НСД «Страж NT» (версия 4.0) имеет сертификат ФСТЭК России №3553 и может применяться при разработке систем защиты информации для одно и многопользовательских автоматизированных систем и информационных систем обработки персональных данных в соответствии с требованиями законодательства Российской Федерации. В первую очередь, если говорить о подсистеме настройки, то рассматривается *«консоль управления.»*

Основной программой настройки и управления системой защиты является программа «Консоль управления». Программа «Консоль управления» предназначена для выполнения администратором системы защиты следующих действий:

- настройка общих параметров системы защиты информации;

- создание ЗПС;
- управление пользователями системы и идентификаторами;
- учет носителей информации и настройка параметров их использования;
- настройку параметров контроля подключенных устройств компьютера;
- работа с журналом событий системы защиты;
- создание и применение сценариев настроек защиты;
- формирование отчетов по настройкам системы защиты;
- тестирование механизмов системы защиты;
- архивирование и восстановление настроек системы защиты.

Далее рассматривается управление пользователями [2]. Чтобы пользователь мог работать в системе, необходимо создать его учетную запись, назначить ей допуск (уровень конфиденциальности), пароль и сформировать для пользователя персональный идентификатор. Только предъявив персональный идентификатор и пароль, пользователь может войти в систему. При входе в Windows система защиты автоматически подставляет имя и домен пользователя, считанные с идентификатора, и его пароль, введенный до загрузки ОС. Полученная идентификационная информация сопоставляется с информацией, хранящейся в базе пользователей, и подсистема идентификации и аутентификации принимает решение о входе пользователя или отказе ему в доступе. При этом информация о пользователях автономных рабочих станций и рабочих станций в составе рабочей группы хранится в локальных базах SAM, тогда как информация о пользователях домена – в базе Active Directory на контроллерах домена. В составе идентификационной информации также присутствуют данные о компьютерах, на которые может входить пользователь.

Чтобы пользователь мог работать на нескольких компьютерах с одним персональным идентификатором и паролем необходимо, во-первых, на каждой

рабочей станции или сервере, не входящих в домен, создать пользователей под одним и тем же именем и назначить им одинаковые пароли. Если компьютеры находятся в домене, необходимо просто создать пользователя в Active Directory. И во-вторых, необходимо сформировать идентификатор пользователя, в котором будет включена информация обо всех необходимых компьютерах.

Управление пользователями на рабочих станциях и серверах в составе рабочей группы, а также в составе домена может осуществляться с единого рабочего места администратора системы защиты, входящего в эту рабочую группу или домен [2].

Управление пользователями и персональными идентификаторами осуществляется с помощью вкладки Пользователи программы Консоль управления, перейдя в которую администратор системы защиты может выполнять следующие функции:

- создание, удаление и переименование пользователей;
- редактирование свойств пользователя;
- просмотр и смена пароля пользователя;
- формирование персональных идентификаторов пользователей;
- просмотр списка идентификаторов пользователя;
- чтение и очистка идентификаторов.

Рассмотрим замкнутую программную среду В целях обеспечения безопасности при работе пользователей в СЗИ «Страж NT» реализован механизм ЗПС. Данный механизм заключается в том, что каждый исполняемый файл системы, необходимый для работы пользователя, должен иметь разрешение на запуск. Для этого служит защитный атрибут – режим запуска, который может иметь следующие значения:

- «Запрещен» (по умолчанию);
- «Приложение»;

- «Сервер-приложение»;
- «Инсталлятор» [2].

Пользователь может запустить программу, хранящуюся в файле, на выполнение, если для данного файла значение режима запуска отличается от значения «Запрещен». Если режим запуска файла имеет значение «Запрещен», запрос на выполнение не будет выполнен. Изменение режима запуска файла может дать только администратор системы защиты. Таким образом, для пользователей формируется ЗПС, при которой пользователь не может запустить программу, для которой не разрешен режим запуска. Различие замкнутых программных сред для разных пользователей осуществляется дискреционным принципом контроля доступа.

Все файлы, для которых значение режима запуска отличается от значения «Запрещен», доступны пользователям только на чтение, что обеспечивает целостность программной среды.

Далее необходимо рассмотреть настройку ЗПС В системе защиты существует возможность автоматизированной настройки ЗПС. Настройка ЗПС осуществляется при помощи вкладки «Настройки программы» «Консоль управления». Для запуска процесса настройки необходимо выбрать пункт меню «Настройки ресурсов» далее «ЗПС». При этом начинается процесс построения дерева папок, длительность которого зависит от параметров компьютера и может занять несколько минут. В результате в появившемся диалоге администратор сможет выбрать папки, которые будут анализироваться при настройке ЗПС.

Если папка отмечена флагом, поиск будет производиться только в этой папке без учёта вложенных папок. При нажатии правой кнопки мыши в области дерева папок, на экране появится контекстное меню. Пункт «Выбрать дочерние», позволяет отметить все папки в указанной папке, вложенные папки отмечены не будут. Пункт «Выбрать все дочерние», позволяет выбрать все

папки в указанной папке, в том числе и все вложенные папки. Пункт «Отменить выбор», снимает флаги со всех вложенных папок. При нажатии кнопки на все исполняемые файлы в отмеченных папках будет установлен режим запуска.

В некоторых случаях в 32-х разрядных ОС стандартные механизмы анализа исполняемых файлов не распознают исполняемый файл. Это происходит в случаях, если программа написана для работы под управлением операционной системы MS-DOS или имеет нестандартный PE-заголовок. Чтобы на такие файлы устанавливался режим запуска, необходимо перед нажатием кнопки установить флаг «Поддержка старых форматов».

Установка флага «Исключить файлы в профилях пользователей» означает, что на исполняемые файлы, находящиеся в папках профилей пользователей, не будет устанавливаться режим запуска [2].

Далее необходимо рассмотреть управление доступом, в частности дискреционный принцип контроля доступа. Для работы с файлами и папками на дисках операционная система MS Windows поддерживает несколько файловых систем, включая FAT, NTFS, CDFS. Между данными файловыми системами много различий, но главное, что только NTFS обеспечивает защиту файлов и папок при локальном доступе. В отличие от MS Windows, дискреционный принцип контроля доступа, реализованный в системе защиты «Страж NT», не зависит от типа файловой системы и поддерживает защиту ресурсов для любых файловых систем. [2]

В рамках дискреционного принципа контроля доступ к защищаемым ресурсам контролируется механизмами системы защиты с помощью разрешений, содержащихся в записях списка контроля доступа. К защищаемым ресурсам компьютера относятся носители информации, папки, файлы, принтеры и устройства. Список контроля доступа может содержать как разрешающие, так и запрещающие записи. Существуют следующие основные разрешения на доступ к ресурсам: «Полный доступ», «Изменение», «Чтение и

выполнение», «Чтение» и «Запись». Каждое из этих разрешений представляет собой логическую группу особых разрешений.

Рассмотрим мандатный принцип контроля доступа Мандатный принцип контроля доступа реализован посредством назначения защищаемым ресурсам, каждому пользователю системы и прикладным программам меток конфиденциальности и сравнения их при запросах на доступ. В качестве меток конфиденциальности выступают:

- для защищаемых ресурсов – гриф секретности;
- для пользователей – уровень допуска;
- для прикладных программ – допуск и текущий допуск [2].

Гриф секретности ресурса представляет собой уровень его конфиденциальности в иерархической классификации. Уровень допуска пользователя определяет максимальный гриф секретности ресурса, доступный пользователю для чтения. Допуск прикладной программы определяет максимальный гриф секретности ресурса, доступный программе для чтения. Текущий допуск прикладной программы представляет собой действующее в конкретный момент времени значение допуска программы. При контроле доступа к защищаемым ресурсам непосредственно сравнению подлежат только значения грифа секретности ресурса и текущего допуска прикладной программы. Уровень допуска пользователя и допуск прикладной программы имеют значение только лишь при установке текущего допуска прикладной программы.

В СЗИ «Страж NT» по умолчанию используются следующие значения меток конфиденциальности в порядке повышения:

- «Несекретно»;
- «Конфиденциально»;
- «Секретно»;
- «Совершенно секретно». [2]

При настройке приложений для работы с различными текущими допусками часто возникает проблема выявления файлов, которые используются для сохранения служебной информации приложения и должны быть доступны для чтения и записи при работе приложения со всеми значениями текущего допуска. Как правило, на такие файлы должен устанавливаться гриф «Без проверки».

Альтернативой указанному методу является включение механизма виртуализации объектов и установка на родительскую папку таких объектов флага виртуализации. При установке на папку флага виртуализации для каждого грифа будет при необходимости создан свой образ исходной папки, на которую будет автоматически перенаправляться запрос при обращении к ней приложения с соответствующим текущим допуском.

Рассмотрим виртуализацию объектов. При настройке приложений для работы с различными текущими допусками часто возникает проблема выявления файлов, которые используются для сохранения служебной информации приложения и должны быть доступны для чтения и записи при работе приложения со всеми значениями текущего допуска. Как правило, на такие файлы должен устанавливаться гриф «Без проверки».

Альтернативой указанному методу является включение механизма виртуализации объектов и установка на родительскую папку таких объектов флага виртуализации. При установке на папку флага виртуализации для каждого грифа будет при необходимости создан свой образ исходной папки, на которую будет автоматически перенаправляться запрос при обращении к ней приложения с соответствующим текущим допуском. Установку флага виртуализации на папки можно выполнить с помощью любого файлового менеджера, например, программы «Менеджер файлов» и только в режиме администрирования. Для установки флага виртуализации необходимо включить режим администрирования, выбрать пункт «Свойства» из контекстного меню выбранных объектов, и в появившемся окне свойств выбрать вкладку «Гриф» и

«режим запуска». Для установки флага виртуализации на папку необходимо установить флаг в поле «Виртуализация объектов.» Если механизм виртуализации объектов выключен, данное поле будет недоступно для изменения. [2]

Рассмотрим управление носителями информации. СЗИ «Страж NT» контролирует доступ ко всем носителям информации, используемым в процессе работы. При подключении носителя информации система защиты проверяет, зарегистрирован ли он в системе. Если носитель является зарегистрированным, к нему будут применяться те правила безопасности, которые ему задал администратор системы защиты. Если носитель не зарегистрирован, к нему будут применяться правила, заданные для группы носителей, к которой он принадлежит.

В СЗИ «Страж NT» поддерживаются следующие типы носителей:

- дискеты;
- CD/DVD диски;
- магнито-оптические диски;
- ленточные накопители;
- жесткие диски;
- съёмные диски. [2]

В процессе установки системы защиты в список зарегистрированных носителей будут добавлены все присутствующие на момент установки носители типа «Жёсткий диск». В дальнейшем администратор системы защиты может поменять свойства зарегистрированных носителей.

Рассмотрим контроль устройств. СЗИ «Страж NT» контролирует доступ к устройствам, присутствующим в компьютере, через подсистему контроля устройств, которая позволяет устанавливать разрешения на различные типы устройств. В соответствии с разрешениями после интерактивного входа пользователя в систему устройства, запрещенные данному пользователю, будут

отключены. При попытке подключить устройство, запрещенное пользователю, подсистема контроля устройств отключит данное устройство. В СЗИ «Страж NT» контролируются следующие типы устройств:

- Bluetooth устройства;
- устройства IEEE 1394;
- инфракрасные порты;
- модемы;
- multifunctional устройства;
- сетевые карты;
- PCMCIA устройства;
- порты (COM и LPT);
- устройства чтения смарткарт;
- устройства USB;
- переносные устройства. [2]

Рассмотрим целостность ресурсов В системе защиты предусмотрен КЦ защищаемых файлов и файлов системы защиты. КЦ файлов может осуществляться автоматически при загрузке операционной системы, при открытии файлов на чтение и по запросу. СЗИ «Страж NT» обеспечивает КЦ файлов по следующим параметрам:

- наличие файла;
- контрольная сумма данных, содержащихся в файле.
- длина файла;
- дата и время последней модификации.

При контроле целостности файлов параметры контроля проверяются в последовательности, приведенной выше. При нарушении какого-либо параметра подсистемой регистрации фиксируется факт нарушения целостности, и дальнейшая проверка не производится. [2]

В рамках этой же подсистемы реализован КЦ исполняемых файлов системы защиты. КЦ на файлы системы защиты устанавливается автоматически при установке системы защиты и его параметры не могут быть изменены.

При обнаружении нарушения целостности файлов, параметры которых контролируются автоматически при загрузке операционной системы, после загрузки рабочего стола у пользователя на экран появляется окно с сообщением. При появлении такого сообщения необходимо открыть журнал событий и проанализировать, у каких файлов и по какой причине нарушена целостность.

Рассмотрим регистрацию событий. В СЗИ «Страж NT» реализована собственная подсистема регистрации событий. Все регистрируемые события включены в следующие категории:

- события контроля целостности;
- события входа в систему;
- события запуска программ;
- события доступа к объектам;
- события действий администратора;
- события управления объектами доступа;
- события управления пользователями;
- события управления носителями;
- события управления устройствами;
- события системы защиты;
- события печати.

В категорию входа в систему включены события успешного входа в систему, а также все ошибки идентификации пользователей. Категория запуска программ включает события успешного запуска процессов, попытки запуска

неразрешенных программ, попытки установки текущего допуска, режима администрирования и автозапуска. Категория доступа к объектам объединяет подключение томов, попытки обращения к защищаемым файлам и папкам, а также установку атрибутов безопасности на файлы. В категорию контроля целостности входят все факты нарушения целостности защищаемых файлов. События из перечисленных выше категорий, а также действия администратора и события системы защиты, регистрируются средствами ядра системы защиты. Остальные категории событий регистрируются в соответствующих подсистемах. [2]

При возникновении какого-либо события регистрируются следующие параметры:

- дата и время;
- код события;
- имя пользователя;
- другие параметры, зависящие от категории события.

Для регистрации событий доступа к защищаемым файлам и папкам в системе защиты предусмотрен специальный атрибут безопасности, который называется «Дополнительный аудит» и может быть установлен как на процесс, так и на любой защищаемый файл или папку.

Теперь рассматриваются сценарии Сценарии настроек системы защиты представляют собой последовательности действий по настройке системы защиты и могут в себе содержать:

- файловые операции;
- операции с пользователями;
- операции с носителями.

Каждый из типов сценариев поддерживает определённые типы действий. Так, сценарии, содержащие «Операции с пользователями» позволяют создавать пользователей. Сценарии типа «Операции с носителями» позволяют

регистрировать носители различных типов. А сценарии типа «Файловые операции» позволяют создавать, удалять, копировать файлы и папки, запускать программы от имени различных пользователей, устанавливать параметры целостности, грифы, параметры запуска и т.д.

В панели сценариев будет отображён список сценариев, расположенных в папке сценариев. Изменить папку, из которой будет читаться список сценариев, можно в окне общих настроек СЗИ. При выборе сценария в основном окне будет представлен список действий выбранного сценария. [2]

Рассмотрим работу с журналами. Подсистема регистрации кроме регистрации запросов на доступ к ресурсам компьютера также обеспечивает их хранение и возможность выборочного ознакомления с регистрационной информацией. Работа с журналом событий осуществляется с помощью вкладки «Журнал событий» программы «Консоль управления», перейдя в которую администратор системы защиты может выполнять следующие функции:

- просмотр списка событий;
- просмотр свойств выбранного события;
- применение фильтра при просмотре списка событий;
- сортировка событий по основным полям;
- поиск событий в журнале по любому из критериев;
- сохранение журнала или отдельной выборки событий;
- очистка журнала. [2]

Рассмотрим терминальный доступ В СЗИ «Страж NT» поддерживаются защитные механизмы при подключении пользователей к терминальному серверу. Если на терминальном сервере установлена система защиты при подключении пользователей к нему выполняется терминальная идентификация пользователей, т.е. запрашивается идентификатор и пароль пользователя. Для успешной идентификации необходимо, чтобы на компьютере-клиенте, с которого происходит подключение, также была установлена СЗИ «Страж NT»

данной версии, а также модули поддержки терминальных подключений. Кроме того, на идентификаторе пользователя должен быть разрешен доступ к терминальному серверу, а имя и пароль пользователя на клиенте и терминальном сервере должны совпадать. Также необходимо убедиться, что на клиенте во время удаленного сеанса будут разрешены локальные смарт-карты. При выполнении всех этих условий идентификационная информация пользователя, записанная на персональном идентификаторе, будет передана на терминальный сервер и считана процедурой терминальной идентификации. [2] После чего будет выдан запрос на ввод пароля пользователя с клавиатуры. В случае успешного ввода пароля произойдет вход пользователя в удаленную сессию на терминальном сервере. После трех неудачных попыток ввода пароля на экран выдается сообщение «Несанкционированный доступ», которое сопровождается звуковой сигнализацией. В журнал регистрации заносится соответствующее сообщение, после чего терминальная сессия завершается. В тех случаях, когда на клиенте терминального сервера по какой-либо причине невозможно установить СЗИ «Страж NT», терминальная идентификация может быть отключена. Для отключения терминальной идентификации требуется ввод специальной терминальной лицензии на определенное количество подключений на терминальном сервере.

Управление терминальными лицензиями осуществляется в программе «Консоль управления» во вкладке «Настройки». [2]

Рассмотрим управление настройками. В СЗИ «Страж NT» существует возможность управлять настройками защищаемых ресурсов и настройками самой системы защиты. Под управлением настройками защищаемых ресурсов понимается сохранение, автоматическое архивирование и восстановление настроек защищаемых ресурсов, таких как: папки и файлы, носители информации, группы устройств. Механизмы управления настройками защищаемых ресурсов будут необходимы при снятии «слепков настроек», например, перед установкой нового программного обеспечения или пакета

обновления операционной системы. Под управлением настройками СЗИ понимается экспорт настроек СЗИ в файл или на другой компьютер и импорт настроек СЗИ из файла. [2]

Формирование отчетов

В СЗИ «Страж NT» предусмотрена возможность создания отчетов о настройках системы защиты. Отчёты могут содержать информацию:

- о пользователях СЗИ;
- об используемых идентификаторах;
- о зарегистрированных носителях;
- о подключенных устройствах;
- об установленных принтерах;
- о настройках защищаемых ресурсов файловой системы. [2]

2.3 Secret Net 7

Программное обеспечение СЗИ Secret Net 7 является системой защиты информации на серверах и рабочих станциях от несанкционированного доступа. Решение работает под управлением MS Windows (Vista, 2000, XP и 2003). Secret Net сочетает в себе необходимые функции защиты информации, средства централизованного управления, инструменты оперативного принятия решений и возможность мониторинга безопасности информационной системы в реальном времени. Тесная интеграция защитных механизмов Secret Net с механизмами управления сетевой инфраструктурой повышает защищенность корпоративной информационной системы.

Secret Net обеспечивает защиту конфиденциальной информации и осуществляет контроль и мониторинг при обработке персональных данных, повышая уровень автоматизации и сокращая административные затраты.

Разные редакции Secret Net позволяют строить эффективную систему защиты информации от НСД в соответствии с потребностями бизнеса:

Автономный вариант – решение, предназначенное для защиты серверов и рабочих станций. Рекомендуется применять при небольшом количестве защищаемых рабочих станций (20-25 компьютеров).

Сетевой вариант – решение, дополненное средствами централизованного управления безопасностью для работы в больших сетях и рекомендованное к применению в сетях с большим количеством рабочих станций.

Основные возможности:

- разграничение доступа к защищаемой информации и устройствам;
- идентификация и аутентификация пользователей.;
- централизованное управление политиками безопасности;
- ведение журналов событий, аудит;
- гарантированное уничтожение данных при их удалении пользователем;
- поддержка терминальных сессий пользователей для платформ Citrix и Microsoft;
- возможность масштабирования;
- управление доступом пользователей к конфиденциальным данным;
- защита от загрузки с внешних носителей;
- контроль аппаратной конфигурации компьютера;
- защита информации в процессе хранения: шифрование файлов, контроль печати конфиденциальной информации и регистрация событий;
- удобство управления и настроек: импорт и экспорт настроек.

В данном разделе рассматривается подсистема настройки СЗИ от НСД Secret Net 7 Организация управления системой защиты. В автономном режиме

функционирования системы Secret Net доступны только локальные функции управления системой.

В сетевом режиме функционирования доступны возможности как локального, так и централизованного управления системой защиты, применяются принципы сетевого администрирования с использованием механизма групповых политик и делегирования административных полномочий. [3]

Рассмотрим централизованное и локальное управление Локальное управление — это управление работой механизмов защиты отдельного компьютера, которое осуществляется администратором безопасности непосредственно на компьютере. Локальное управление используется в тех случаях, когда возможности централизованного управления для отдельного компьютера недоступны или нецелесообразны. Например, локальное управление применяется, если требуется обеспечить безопасную работу локальных пользователей компьютера. Программные средства для локального управления установлены по умолчанию и могут использоваться пользователями, входящими в локальную группу администраторов компьютера.

Централизованное управление параметрами Secret Net осуществляется администратором безопасности со своего рабочего места. Для этих целей может использоваться любой компьютер сети с установленными средствами централизованного управления. [3]

В качестве средств централизованного управления параметрами групповых политик и параметрами доменных пользователей могут использоваться:

- стандартные средства централизованного управления ОС Windows;
- средства, входящие в состав ПО системы Secret Net: программа оперативного управления и программа управления пользователями.

Средства управления параметрами групповых политик и параметрами доменных пользователей можно использовать по отдельности (только стандартные средства Windows или только средства системы Secret Net) или комбинированно. Для централизованного управления параметрами механизмов контроля целостности и ЗПС используется программа «Контроль программ и данных» в централизованном режиме работы. Программа входит в состав ПО системы Secret Net.

Рассмотрим использование групповых политик. В сетевом режиме функционирования системы Secret Net для централизованной настройки и применения параметров безопасности на защищаемых компьютерах могут использоваться групповые политики. Заданные параметры объектов групповых политик хранятся в Active Directory и применяются без учета значений, указанных для тех же параметров в локальной политике безопасности компьютера.

Параметры системы Secret Net могут быть заданы в групповых политиках домена, организационного подразделения и сервера безопасности. Соответственно эти параметры будут применяться на компьютерах, входящих в домен, включенных в организационное подразделение или подчиненных серверу безопасности. При этом действуют приоритеты применения групповых политик. Наименьший приоритет имеют параметры политики безопасности домена, заданные в стандартных оснастках ОС Windows. Эти параметры применяются на компьютерах домена, если отсутствуют другие значения в групповых политиках более высокого уровня. [3]

В системе Secret Net могут использоваться следующие групповые политики в порядке возрастания приоритета применения параметров:

- политика безопасности домена, заданная в стандартных оснастках ОС Windows;

- политика организационного подразделения, заданная в стандартных оснастках ОС Windows, — для всех компьютеров, входящих в это организационное подразделение;

- политика домена, заданная в программе оперативного управления системы Secret Net;

- политика организационного подразделения, заданная в программе оперативного управления системы Secret Net, — для всех компьютеров, входящих в это организационное подразделение;

- политика, заданная для сервера безопасности в программе оперативного управления системы Secret Net, — применяется на всех компьютерах, подчиненных этому серверу безопасности. [3]

За счет использования разных групповых политик можно реализовать централизованное управление параметрами с учетом особенностей информационной системы. Например, можно настроить общие параметры для всех компьютеров в политике домена и дополнительно указать значения отдельных параметров в политиках организационных подразделений. Это позволит применять на компьютерах различных организационных подразделений единые общие параметры и при этом задать специфические значения для компьютеров отдельных подразделений.

В сетевом режиме функционирования системы Secret Net можно делегировать полномочия для администратора безопасности. Делегирование подразумевает возложение некоторых функций по настройке и управлению работой механизмов защиты на пользователей, не являющихся членами доменной группы администраторов. При этом настройка и управление будут осуществляться только в рамках определенных организационных подразделений созданных внутри домена.

Процедуру делегирования следует выполнять в случае, если хранилище объектов централизованного управления Secret Net размещается в базе данных

доменных служб Active Directory. Если хранилище объектов размещается вне AD — достаточно включить администратора безопасности в доменную группу Group Policy Creator Owners. [3]

Управление персональными идентификаторами

Персональный идентификатор — устройство для хранения информации, необходимой при идентификации и аутентификации пользователя. В идентификаторе могут храниться ключи для усиленной аутентификации пользователя.

В Secret Net могут использоваться персональные идентификаторы eToken, iKey, Rutoken, JaCarta, ESMART или идентификаторы iButton.

Персональный идентификатор выдается пользователю администратором. Один и тот же персональный идентификатор не может быть присвоен нескольким пользователям одновременно. При этом одному пользователю можно присвоить несколько идентификаторов. Если используется ПАК «Соболь» в режиме интеграции с Secret Net, максимально возможное количество присвоенных идентификаторов для одного пользователя — 32.

Администратор безопасности может выполнять следующие операции с персональными идентификаторами:

Инициализация идентификатора — Форматирование, обеспечивающее возможность использования идентификатора в системе Secret Net. Инициализация требуется, когда в персональном идентификаторе по каким-либо причинам была нарушена или отсутствует структура данных. Форматированию подлежат также и сменные носители, предназначенные для хранения ключей [3]

Присвоение идентификатора — Добавление в базу данных Secret Net сведений о том, что пользователю принадлежит персональный идентификатор данного типа с уникальным серийным номером

Отмена присвоения идентификатора — Удаление из базы данных Secret Net информации о принадлежности данного персонального идентификатора данному пользователю. Далее для простоты эту операцию будем называть «удаление идентификатора»

Включение режима хранения пароля в идентификаторе — Добавление в базу данных Secret Net сведений о включении для пользователя режима хранения пароля в идентификаторе. Одновременно с этой операцией выполняется запись пароля в идентификатор. После включения режима пароль пользователя при входе в систему не вводится с клавиатуры, а считывается из идентификатора

Отключение режима хранения пароля в идентификаторе — Операция, противоположная предыдущей. Одновременно с отключением режима хранения выполняется удаление пароля из памяти персонального идентификатора. Идентификатор остается закрепленным за пользователем

Включение и отключение режима разрешения входа в ПАК «Соболь» — При включенном режиме пользователю разрешено использовать для входа в ПАК «Соболь» идентификатор, присвоенный в системе Secret Net

Запись и удаление ключей для усиленной аутентификации — Используется для хранения в идентификаторе (или на сменном носителе) ключей для усиленной аутентификации пользователя

Проверка принадлежности — С помощью этой операции администратор безопасности может проверить, кому из пользователей присвоен данный персональный идентификатор [3]

Для защиты доступа к устройствам компьютера используются механизм контроля подключения и изменения устройств и механизм разграничения доступа к устройствам. Работа этих механизмов взаимосвязана. Механизм контроля подключения и изменения устройств предназначен для обнаружения и реагирования на изменения аппаратной конфигурации компьютера, а также

для поддержания в актуальном состоянии списка устройств компьютера. По списку устройств с помощью второго механизма выполняется разграничение доступа пользователей к устройствам. Часть функций разграничения доступа к устройствам реализуется с использованием механизма полномочного управления доступом. Защита доступа к принтерам реализуется механизмом контроля печати.

Для представления множества устройств, установленных или подключаемых к защищаемым компьютерам, используется иерархическая схема списка устройств. Устройства группируются в классы, а классы, в свою очередь, включены в состав групп. Группы являются элементами объединения верхнего уровня. Количество групп фиксировано. Предусмотрены следующие группы:

«Локальные устройства» — объединяет фиксированные устройства компьютера, для которых не предполагается ограничивать подключение (например, последовательные и параллельные порты, процессоры, оперативная память);

– «Устройства USB» — объединяет устройства, подключаемые к шине USB;

– «Устройства PCMCIA» — объединяет устройства, подключаемые к шине PCMCIA;

– «Устройства IEEE1394» — объединяет устройства, подключаемые к шине IEEE1394;

– «Устройства Secure Digital» — объединяет устройства, подключаемые к шине Secure Digital;

– «Сеть» — объединяет устройства, являющиеся сетевыми интерфейсами (адаптеры). Если сетевым интерфейсом является нефиксированное подключаемое устройство, такое устройство может также присутствовать и в другой группе. Это дает возможность настроить реакцию

системы на подключение устройства до его регистрации в качестве сетевого интерфейса. [3]

Некоторые классы допускают дополнительное разбиение устройств по моделям. Модели объединяют устройства с одинаковыми идентификационными кодами, присвоенными производителем. В списке устройств присутствуют predetermined модели — например, модели электронных идентификаторов.

Также в список можно добавлять модели на основе имеющихся устройств, если в этих устройствах производителем были указаны идентификационные коды. В дальнейшем при обнаружении нового устройства с такими же идентификационными кодами это устройство автоматически будет добавлено в качестве экземпляра к той же модели. За счет этого можно управлять одинаковыми устройствами без необходимости настройки параметров каждого устройства по отдельности.

Для объектов каждого уровня (группа, класс, модель, устройство) определен набор параметров, с помощью которых настраиваются механизмы контроля подключения и изменения устройств, разграничения доступа к устройствам, теневого копирования и полномочного управления доступом. Иерархия списка устройств в большинстве случаев позволяет выполнять настройку как на уровне отдельного устройства, так и на уровне классов и групп.

На компьютере список устройств создается сразу после установки клиентского ПО системы Secret Net при первой загрузке ОС. Этот список устройств принимается как эталонная конфигурация компьютера. Список устройств отображается в локальной политике безопасности и хранится в локальной базе данных системы Secret Net. [3]

В сетевом режиме функционирования системы защиты можно создать список устройств в групповой политике. После создания список устройств

состоит из групп, классов и predetermined моделей устройств. При необходимости в список можно добавить и конкретные устройства. Заданные параметры в этом списке устройств хранятся и распространяются в домене в составе доменных (групповых) политик.

Настройка параметров использования принтеров осуществляется в отдельном списке «Принтеры». Параметры могут применяться по умолчанию при печати на любые принтеры или могут быть заданы для отдельных принтеров.

Печатающие устройства, представленные в списке принтеров, могут также присутствовать как устройства и в списке устройств. Это дает возможность настроить реакцию системы на подключение устройства до его регистрации в качестве принтера.

На компьютере список принтеров создается сразу после установки клиентского ПО системы Secret Net. Список принтеров изначально состоит из одного элемента «Настройки по умолчанию». Параметры использования принтеров, заданные для этого элемента, применяются ко всем принтерам, кроме тех, которые в явном виде присутствуют в списке принтеров. Добавление принтеров в список политики осуществляется с помощью специальной программы-мастера.

Явно заданные параметры для конкретных принтеров имеют приоритет перед параметрами элемента «Настройки по умолчанию». Список принтеров локальной политики безопасности хранится в локальной базе данных системы Secret Net.

В сетевом режиме функционирования системы защиты можно задать параметры использования принтеров в групповой политике. Действия для формирования списка и настройки параметров выполняются так же, как и в локальной политике безопасности. Заданные параметры в этом списке

принтеров хранятся и распространяются в домене в составе доменных (групповых) политик. [3]

Дискреционное управление доступом к каталогам и файлам

При настройке дискреционного разграничения доступа пользователей к каталогам и файлам на локальных дисках выполняются действия:

- Предоставление привилегии для изменения прав доступа на любых ресурсах;
- Назначение администраторов ресурсов;
- Настройка регистрации событий и аудита операций с ресурсами.

В механизме дискреционного управления доступом предусмотрена возможность для привилегированных пользователей изменять права доступа на любых каталогах и файлах локальных дисков независимо от установленных прав доступа к самим ресурсам. Для этого пользователю должна быть предоставлена привилегия «Дискреционное управление доступом: Управление правами доступа». Привилегия, в частности, позволяет назначить администраторов ресурсов, которые в дальнейшем смогут настраивать права доступа к ресурсам для остальных пользователей.

По умолчанию привилегией на управление правами доступа обладают пользователи, входящие в локальную группу администраторов.

Администраторы ресурсов в механизме дискреционного управления доступом могут изменять права доступа других пользователей к определенным каталогам и файлам на локальных дисках. Администратором ресурса считается пользователь, для которого установлено разрешение на операцию «Изменение прав доступа» в параметрах доступа к ресурсу. [3]

Изменение перечня регистрируемых событий Для отслеживания произошедших событий, связанных с работой механизма дискреционного управления доступом к каталогам и файлам, необходимо выполнить настройку

регистрации событий. Для этого следует указать, какие события категории «Дискреционный доступ» должны регистрироваться в журнале Secret Net. [3]

Механизм КЦ предназначен для слежения за неизменностью содержимого ресурсов компьютера. Действие этого механизма основано на сравнении текущих значений контролируемых параметров проверяемых ресурсов и значений, принятых за эталон. Эталонные значения контролируемых параметров определяются или рассчитываются при настройке механизма. В процессе контроля при обнаружении несоответствия текущих и эталонных значений система оповещает администратора о нарушении целостности ресурсов и выполняет заданное при настройке действие, например, блокирует компьютер, на котором нарушение обнаружено.

Механизм ЗПС предназначен для ограничения использования ПО на компьютере. Доступ разрешается только к тем программам, которые необходимы пользователям для работы. Для каждого пользователя определяется перечень ресурсов, в который входят разрешенные для запуска программы, библиотеки и сценарии. Попытки запуска других ресурсов блокируются, и в журнале безопасности регистрируются события несанкционированного доступа НСД. [3]

Для настройки механизмов КЦ и ЗПС используется программа «Контроль программ и данных», входящая в состав клиентского ПО системы Secret Net. В данной главе рассматриваются методы работы с программой.

Программа управления КЦ-ЗПС располагает как автоматическими, так и ручными средствами формирования элементов модели данных. Ручные методы можно использовать на любом уровне модели для формирования и модификации объектов и связей. Автоматические методы предпочтительнее при работе с большим количеством объектов, однако они требуют более тщательного контроля результатов. Для создания небольших фрагментов модели могут быть использованы ручные методы, что делает процесс более

контролируемым и позволяет избежать случайных ошибок. В общем случае наиболее типичный путь состоит в комбинации этих двух методов. [3]

Присвоенные пользователям персональные идентификаторы могут использоваться для терминального входа в подключениях удаленного доступа. Для этого на компьютере, который является терминальным сервером, должен быть включен любой из следующих режимов идентификации механизма защиты входа:

- «Смешанный» (включен по умолчанию);
- «Только по идентификатору».

При этом в средствах подключения к удаленному рабочему столу (Remote Desktop Connection) версии 6.0 и выше (в составе ОС Windows Vista и выше) по умолчанию требуется предварительная аутентификация пользователя. Предварительная аутентификация осуществляется путем ввода учетных данных пользователя (имя и пароль) до подключения к терминальному серверу. Из-за этого проявляются следующие особенности установки соединения:

- Если на терминальном сервере включен режим идентификации «Смешанный» — после предварительной аутентификации на терминальном клиенте сразу осуществляется терминальный вход по указанным учетным данным пользователя. Терминальный сервер не ожидает предъявление идентификатора.

- Если на терминальном сервере включен режим идентификации «Только по идентификатору» — при удаленном подключении сначала выполняется предварительная аутентификация (пользователь вводит имя и пароль для инициирования подключения), а затем при соединении с терминальным сервером пользователю необходимо предъявить свой персональный идентификатор.

При отключенной предварительной аутентификации обеспечивается вход пользователя в терминальную сессию по идентификатору без предварительного запроса имени и пароля [3].

По умолчанию в журнале Secret Net регистрируются все возможные события, кроме событий категории «Контроль приложений» и некоторых событий категорий «Контроль целостности» и «Дискреционный доступ».

Функцию теневого копирования можно отключить для всех устройств следующих типов:

- устройства, подключаемые к системе в качестве дисков;
- принтеры.

Если функция теневого копирования включена, будут действовать параметры, заданные соответственно для устройств и/или принтеров. [3]

В журнале Secret Net могут регистрироваться события запуска и завершения работы приложений (процессов) для обеспечения возможности аудита отслеживания процессов средствами системы защиты. Регистрация может выполняться в следующем объеме:

- события, относящиеся к работе только тех приложений, запуск которых выполнен пользователем компьютера;
- события запуска и завершения для всех процессов системы — не только пользовательских приложений, но и системных. [3]

Механизм полномочного управления доступом обеспечивает разграничение доступа пользователей к конфиденциальным ресурсам. Ресурс считается конфиденциальным, если ему назначена категория конфиденциальности, отличная от категории для общедоступной информации (по умолчанию — «неконфиденциально»). Категорию можно назначить для следующих ресурсов:

- локальные физические диски (кроме диска с системным логическим разделом) и любые устройства, включаемые в группы устройств USB, PCMCIA, IEEE1394 или Secure Digital;

- каталоги и файлы на дисках с файловой системой NTFS.

Для сетевых интерфейсов можно указать уровни конфиденциальности сессий, в которых разрешается функционирование этих интерфейсов (используется в режиме контроля потоков).

Для принтеров можно указать категории конфиденциальности документов, разрешенных для печати. [3]

Доступ пользователя к конфиденциальной информации осуществляется в соответствии с его уровнем допуска.

Категория конфиденциальности является атрибутом ресурса. По умолчанию в механизме полномочного управления доступом используются следующие категории конфиденциальности:

- «неконфиденциально»;
- «конфиденциально»;
- «строго конфиденциально».

При необходимости можно увеличить количество используемых категорий и задать для них названия в соответствии со стандартами, принятыми в вашей организации. Максимально возможное количество категорий — 16.

После установки клиентского ПО системы Secret Net всем каталогам и файлам на локальных дисках компьютера назначена категория «неконфиденциально» (если ресурсы не имеют ранее присвоенных категорий конфиденциальности).

Повышение категорий конфиденциальности нужных файлов осуществляется пользователями в пределах своих уровней допуска. При этом понижать категории конфиденциальности ресурсов, а также повышать

категории каталогов разрешено только пользователям, которым предоставлена привилегия на управление категориями конфиденциальности.

Для устройств, которым можно назначить категорию конфиденциальности или выбрать допустимые уровни конфиденциальности сессий, по умолчанию включен режим доступа «Устройство доступно без учета категории конфиденциальности» или «Адаптер доступен всегда». Для принтеров по умолчанию включен режим разрешения печати документов любой категории конфиденциальности. Данные режимы разрешают использование устройств и принтеров независимо от уровня допуска пользователя. Назначение устройствам и принтерам нужных категорий или уровней конфиденциальности осуществляется администратором. [3]

2.4 Аккорд-Win 64 (TSE)

Основные характеристики:

Собственная система разграничения доступа (мандатный и дискреционный методы контроля) - действия, разрешенные прикладным ПО, но запрещенные АККОРДОМ - будут запрещены пользователю.

Комплексная защита терминальной сессии обеспечивается тогда и только тогда, когда пользователь может работать только с защищенного терминала и только с защищенным терминальным сервером. Для этого в момент создания терминальной сессии со стороны терминального сервера необходимо аутентифицировать не только пользователя, но и терминал, а со стороны терминала необходимо убедиться в том, что терминальный сервер действительно тот, с которым должен работать пользователь. Это возможно только при наличии активных СЗИ и на терминале, и на сервере. Таким образом, для защиты терминальной сессии необходимо установить комплекс не только на терминальный сервер, но и на терминалы.

Возможность использовать уже установленную связь (на протоколах RDP и ICA) между сервером и терминалом, а не устанавливать новую.

В течение всего сеанса работы пользователя ведется подробный журнал событий, в котором фиксируются все действия пользователя на терминальном сервере.

Программное обеспечение комплекса позволяет администратору безопасности информации описать любую не противоречивую политику безопасности на основе наиболее полного набора атрибутов.

меток доступа, которые могут быть поименованы как уровни секретности либо другим, более удобным образом (количество меток допуска может достигать шестнадцати);

Возможно использование вместо пароля (или одновременно с паролем) биометрической аутентификации пользователя.

Сильной стороной продукта является возможность контроля печати, как на сетевых принтерах, так и на локальных, с протоколированием вывода документов на печать и их маркировки. Данные настройки работают при печати документов из любого прикладного программного обеспечения, предусматривающего возможность вывода документа на печать (не только Microsoft Office). В качестве маркера может выступать, например, гриф секретности документа, имя пользователя, имя принтера, имя документа и другая служебная информация. Рассмотрим подсистему настройки СЗИ от НСД Аккорд-Win32/64

Подсистема управления доступом предназначена для защиты СВТ от посторонних пользователей, управления доступом к объектам доступа и организации совместного их использования зарегистрированными пользователями в соответствии с установленными правилами разграничения доступа . [4]

Защита от посторонних пользователей обеспечивается процедурами идентификации (сравнение предъявленного Идентификатора с перечнем зарегистрированных на СВТ) и аутентификации (подтверждение принадлежности данного идентификатора данному пользователю) с защитой от раскрытия пароля.

Для идентификации/аутентификации пользователей используются персональные идентификаторы DS-1992-1996 (Touch memory-«Память касания»), USB идентификаторы ПСКЗИ ШИПКА, или смарт-карты eTokenPro.

В комплексе «Аккорд» реализованы принципы дискреционного и мандатного управления доступом. При использовании дискреционного управления зарегистрированному пользователю устанавливаются права доступа по принципу регистрации «белого списка» разрешенных к запуску программ (задач) и данных, а так же «черного списка» запрещенных ресурсов, которые прописываются в ПРД. При использовании мандатного управления пользователю (субъекту) устанавливается уровень доступа, а объекту (данным или задаче) присваивается метка доступа (гриф). При запросе пользователя на доступ к объекту, в зависимости от уровня полномочий пользователя, разрешается или запрещается запрошенный тип доступа. Возможно использование одновременно двух механизмов доступа.

Настройка подсистемы разграничения доступом комплекса осуществляется администратором БИ с использованием программы ACED32.

Программа ACED32.EXE – редактор параметров (атрибутов) доступа пользователей, используемых в комплексе СЗИ НСД «Аккорд-Win32» v.4.0 (далее ПАК СЗИ НСД «Аккорд», комплекс «Аккорд» или комплекс) дискреционного и мандатного механизмов доступа субъектов (пользователей) к объектам СВТ или АС – предназначена для администрирования подсистемы разграничения доступом комплекса. [4]

Программа используется администратором БИ системы защиты информации на базе комплекса (или субъектами доступа, наделенными правами администратора) при установке и эксплуатации комплекса для описания (определения пользователям) принятых в организации (учреждении и т.п.) правил разграничения доступа (ПРД) в соответствии с полномочиями пользователей.

СЗИ НСД «Аккорд» поддерживает два типа управления правилами разграничения доступа:

- дискреционный механизм ПРД;
- мандатный механизм ПРД. [4]

При установке дискреционных ПРД могут использоваться атрибуты доступа. Атрибуты доступа к операции с файлами:

- разрешение на открытие файлов только для чтения;
- разрешение на открытие файлов для записи;
- разрешение на создание файлов на диске;
- разрешение на удаление файлов;
- разрешение на переименование файлов;
- видимость файлов. Позволяет делать существующие файлы невидимыми для пользовательских программ. Доступ возможен только по полному пути в формате Windows NT. Этот параметр имеет более высокий приоритет, чем R,W,D,N,O.E эмуляция разрешения на запись информации при открытии файла. Этот параметр имеет более низкий приоритет, чем W (открыть для записи). Параметр может пригодиться в том случае, если программа по умолчанию открывает файл для чтения/записи, а мы хотим разрешить пользователю только просмотр файла.

Атрибуты доступа к операции с каталогом:

- создание каталогов на диске (или подкаталогов в каталоге, для которого устанавливается атрибут);
- удаление каталогов на диске (или подкаталогов в каталоге, для которого устанавливается атрибут);
- разрешение перехода в этот каталог;
- переименование каталога. В ОС Windows, например, удаление папки в «корзину» – это, на самом деле, переименование каталога.

Установка доступа к объектам с использованием мандатного метода контроля ПРД [4].

Мандатный механизм доступа реализуется по следующему правилу: если уровень доступа пользователя (субъекта) выше или равен метке доступа каталога, файла, сетевого ресурса (объекта) то доступ к объекту предоставляется данному субъекту. Если при этом установлены дискреционные ПРД, то операции, которые пользователь может выполнять с разрешенным объектом (чтение, запись, удаление и пр.), определяются атрибутами дискреционного доступа. По умолчанию всем объектам присваивается самый низкий уровень – общедоступно. Для объекта можно изменить только два параметра – уровень доступа и наследование прав доступа. В мандатном механизме доступа СЗИ «Аккорд-Win32» реализована весьма важная с точки зрения безопасности и создания ИПС (изолированной программной среды) функция – это мандатный доступ к объектам со стороны такого субъекта, как процесс (задача), который загружен в оперативную память СВТ. Часто в рамках работы одного процесса создается другой процесс, аналогичный первому. При этом между двумя процессами используется одна и та же среда окружения. В таком случае первый процесс называется родительским, а второй – дочерним.

Флаг «Применить для дочерних процессов» предназначен для того, чтобы при присвоении родительскому процессу определенного уровня доступа дочерним процессам автоматически присваивался такой же уровень доступа,

как и у родительского. Это сделано с целью исключения некорректной работы родительского процесса вследствие отсутствия нужного уровня доступа одного из дочерних процессов.

Администратор может для некоторых процессов установить флаг «Разрешено понизить пользователю». Если этот флаг установлен, то при старте такого процесса выводится окно выбора текущего уровня процесса (конечно, при этом уровень доступа можно выбирать только с понижением). Это дает возможность пользователю в одном сеансе работать с документами разных грифов секретности с помощью одной программы, того же Winword, например, но четко соблюдать правило запрета на «понижение» метки. В реализации процедуры разграничения доступа СЗИ «Аккорд-Win32» исполняемый файл может выступать и как объект, и как субъект. Файл на жестком диске – это объект, которому установлена метка доступа и запустить файл на исполнение может пользователь с соответствующим уровнем доступа. [4]

После запуска процесса он уже как субъект имеет установленный уровень доступа к объектам. В такой системе атрибутов возможна реализация такой политики безопасности, когда обработка объектов с определенной меткой доступа возможна только с помощью процессов соответствующего уровня доступа. Управление потоками информации осуществляется по следующему алгоритму:

- конкретному процессу запись информации разрешена только в том ресурсе, чья метка доступа равна уровню доступа процесса;
- все ресурсы с более низкой меткой доступа открыты для этого процесса только на чтение и запуск программ (атрибуты RVOX).

Таким образом, пользователь не может понизить уровень секретности документа, т.е. скопировать секретный документ в несекретную папку с помощью «секретного» процесса, а для всех процессов, которые не имеют соответствующего уровня, объект «секретно» не доступен.

Программное обеспечение комплекса СЗИ НСД «Аккорд» содержит модули, которые обеспечивают выполнение защитных функций при работе терминального сервера. В качестве серверного ПО может использоваться Windows NT/2000/2003/2008 Terminal Server, в стандартной конфигурации, или с установленным Citrix Metaframe. Установка программного обеспечения на жесткий диск выполняется стандартным образом, только в программе установки включается флаг «Поддержка Terminal Server». При этом различия проявляются только в программе настройки комплекса. Для начала необходимо выбрать протокол виртуального канала, по которому будет осуществляться связь с терминалами. «Аккорд» поддерживает протокол RDP для Windows Terminal Server и ICA для Citrix Metaframe. [4]

Необходимо выбрать хотя бы один протокол, но возможна работа одновременно по двум протоколам. Все остальные настройки правил разграничения доступа на сервере не отличаются от стандартных. Администратор создает пользователя, регистрирует его идентификатор, назначает пароль и правила доступа к ресурсам, которые находятся на жестком диске терминального сервера. Особенность администрирования на терминальном сервере заключается в том, что терминальные пользователи должны регистрироваться в отдельной группе, которая будет синхронизироваться не только с группой Users, но и с группой Remote Desktop Users. Если пользователи уже зарегистрированы в контроллере домена, то возможен вариант, когда синхронизация с базой АМДЗ и базой NT отключается, а сохраняется список только в файле. На терминальном сервере монитор безопасности СЗИ «Аккорд» функционирует в многопользовательском и многозадачном режиме, т.е. для каждого сеанса терминального пользователя выполняется индивидуальная политика работы с ресурсами сервера, основанная на сертифицированных механизмах дискреционного и мандатного доступа. В том случае, когда сформирована ИПС (изолированная программная

среда), то и набор исполняемых модулей жестко регламентирован для каждого пользователя. [4]

Реализованная в СЗИ «Аккорд» процедура динамического контроля целостности существенно усиливает стойкость защиты, т.к. исполняемый модуль, включенный в список контроля, проверяется непосредственно перед каждым запуском, что гарантирует неизменность среды во время всего сеанса работы.

Подсистема регистрации и учета предназначена для регистрации в системном журнале событий, обрабатываемых комплексом СЗИ НСД «Аккорд-АМДЗ» и подсистемой разграничения доступа «Аккорд-Win64» v.5.0. При регистрации событий в системном журнале указываются:

- дата и время события;
- имя пользователя, осуществляющего регистрируемое действие;
- действия пользователя (сведения о входе/выходе пользователя в/из системы, запуске программ, фактах НСД и другие события.);

В СЗИ осуществляется регистрация следующих событий;

- использование идентификационного и аутентификационного механизма;
- запрос на доступ к защищаемому ресурсу (открытие файла, запуск программы и т.д.);
- создание и уничтожение объекта;
- действия по изменению ПРД.

Для каждого из этих событий должна регистрироваться следующая информация:

- дата и время;
- субъект, осуществляющий регистрируемое действие;

- тип события (если регистрируется запрос на доступ, то следует отмечать объект и тип доступа);
- успешно ли осуществилось событие (обслужен запрос на доступ или нет).

КСЗ содержит средства выборочного ознакомления с регистрационной информацией, а также регистрировать все попытки доступа и действия выделенных пользователей. [4]

Подсистема контроля целостности предназначена для исключения несанкционированных модификаций (как случайных, так и злоумышленных) конфигурации технических средств СВТ, программной среды, обрабатываемой информации, обеспечивая при этом защиту СВТ от внедрения программных закладок и вирусов.

КЦ в комплексе реализуется:

- проверкой целостности конфигурации технических средств СВТ перед каждым сеансом работы пользователя;
- проверкой целостности назначенных для контроля системных файлов, пользовательских программ и данных;
- исключением возможности использования СВТ без контроллера комплекса;
- механизмом создания изолированной программной среды, запрещающей запуск неразрешенных программ. [4]

Функционирование подсистемы обеспечения целостности в комплексах СЗИ НСД семейства «Аккорд» основано на использовании следующих механизмов:

- при проверке на целостность вычисляется контрольная сумма файлов и сравнивается с эталонным (контрольным) значением, хранящимся в базе данных пользователей. Эти данные заносятся в энергонезависимую память

контроллера комплекса при регистрации пользователя и могут изменяться в процессе эксплуатации СВТ;

- для исключения фактов не обнаружения модификации файла используется сложный алгоритм расчета контрольных сумм.
- защита от модификации программы расчета контрольной суммы обеспечивается тем, что она хранится в памяти контроллера комплекса;
- при контроле целостности индивидуального списка файлов пользователя результирующая КС хранится на жестком диске, но в алгоритме расчета используется ключ пользователя, записанный в идентификаторе;
- секретный ключ пользователя формируется из последовательности случайных чисел и записывается в идентификатор пользователя при регистрации. Этот ключ используется при выработке КС и исключает возможность несанкционированной модификации файлов из индивидуального списка контролируемых файлов.

Комплекс СЗИ НСД «Аккорд-Win32» v.4.0 позволяет контролировать целостность файлов по индивидуальному списку, созданному администратором для каждого пользователя (или группы). Предусмотрены два режима контроля:

- «статический» - это КЦ любых файлов, расположенных на жестком диске в момент начала сеанса пользователя и обновление контрольных сумм при завершении сеанса работы пользователя;
- «динамический» - это контроль исполняемых модулей перед их загрузкой в оперативную память СВТ. [4]

На первом этапе формируется список файлов, для которых будет рассчитана контрольная сумма (КС). Возможен выбор отдельного файла, или всех файлов из выбранного каталога. Пользоваться возможностями контроля целостности контейнера объектов следует по принципу «разумной достаточности». Можно, например, установить полный контроль на папку Windows, но следует понимать, что время расчета хэш-функции нескольких

тысяч файлов будет значительным, да к тому же пользователь не сможет нормально работать на таком «защищенном» компьютере. Операционная система при работе создает некоторое количество временных файлов и при каждом новом сеансе будет выявлено нарушение целостности. [4]

В то же время контроль контейнера объектов может быть эффективным, когда нужно отследить целостность и неизменность набора данных, необходимых для выполнения технологического процесса обработки информации. Процедура контроля будет выявлять не только изменение контрольных сумм отдельных файлов, но также изменение состава ПО, т.е. появление новых файлов, которые изначально в состав пакета не входили.

На втором этапе осуществляется установка режимов контроля целостности.

Выбор режимов осуществляется установкой флагов в нижней панели окна. Возможны следующие варианты:

- «до запуска системы» - КЦ до запуска операционной системы;
- «с подтверждением» - запрос подтверждения контроля целостности до запуска ОС (пользователь может отказаться от выполнения процедуры контроля);
- «при выходе из системы» - обновление КС после завершения сеанса работы пользователя;
- «с подтверждением» - запрос подтверждения обновления КС после завершения сеанса работы;
- «по времени, через» - КЦ в рамках сеанса пользователя по истечении заданного интервала времени. Если установлено значение 0, то процедура контроля целостности по времени не выполняется. Если установлено отличное от нуля значение интервала времени, то процедура контроля целостности осуществляется по его истечении. [4]

На третьем этапе производится расчет КС выбранных файлов. В процессе расчета запрашивается идентификатор данного пользователя. В алгоритме расчета используется ключ, записанный в идентификатор при регистрации пользователя. Тем самым исключается возможность подделки результирующей КС при несанкционированном изменении файлов.

Эта операция выполняется при каждом запуске процесса (исполняемого модуля). Список контролируемых объектов можно задавать как для отдельного пользователя, так и для группы. В этом случае контроль будет выполняться для любого пользователя из группы. Как для статического, так и для динамического режима контроля возможна загрузка списка контролируемых файлов из специального файла. После того, как файлы будут добавлены в соответствующий список контроля, выполняется расчет контрольных сумм файлов. После выполнения расчета список файлов с контрольными суммами можно сохранить. Этот файл можно использовать на других защищаемых СВТ с идентичным составом прикладного ПО. [4]

2.5 Вывод

Исходя из анализа данных технических средств, можно сделать вывод, что все они имеют практически одинаковую структуру. А именно подсистемы: ЗПС, контроля целостности, регистрации и учета, управления доступом, аутентификации и идентификации и другие. Это обусловлено тем, что рассматриваемые СЗИ от НСД являются сертифицируемыми, и удовлетворяют техническим требованиям ФСТЭК. Различие данных технических решений заключаются лишь в реализации данных подсистем и в использовании дополнительных функций.

3 Постановка проблем проектирования подсистемы настройки средств защиты информации.

3.1 Особенности существующих на рынке средств защиты информации от несанкционированного доступа и их подсистем настройки

При каждой настройке средства защиты информации от несанкционированного доступа к конкретной информационной системе, администратор сталкивается с проблемой выбора защищаемых объектов ИС. На основе анализа подсистем настройки в существующих на рынке средствах защиты информации от несанкционированного доступа, было определено два основных типа настройки СЗИ от НСД:

- шаблонная;
- выборочная.

Шаблонная настройка представляет с собой настройку средства защиты информации от несанкционированного доступа при помощи файла с готовыми конфигурациями. Файл может быть создан разработчиком под конкретную ОС, также есть возможность импортировать настройки с существующей защищенной ИС. Использование шаблонов дает возможность в значительной мере сократить время настройки СЗИ. Для ограничения полномочий администратора ИБ, разработчики в целях безопасности могут использовать шаблон настройки без возможности редактирования.

Выборочная настройка представляет собой пошаговую настройку средства защиты информации от несанкционированного доступа. Основным преимуществом данного типа является гибкость настройки средства защиты информации от несанкционированного доступа с учетом всех особенностей информационных систем в конкретных организациях.

3.2 Проблемы администрирования средств защиты информации от несанкционированного доступа

Проблема администрирования при шаблонной настройке заключается в том, что при данном способе невозможно гибко настроить средство защиты информации под особенности информационных систем конкретных организаций, что может стать причиной ограничения функционала данного СЗИ. Но зачастую разработчики для максимального привлечения аудитории на рынке информационной безопасности дают возможность гибкой настройки СЗИ от НСД. Примером может являться импорт настроек с существующей защищенной ИС. При импортировании существует функция редакции настроек СЗИ на данном компьютере, что позволяет гибко настроить данное СЗИ.

Метод выборочной настройки имеет ряд недостатков, одними из которых является трудоемкость и затраты рабочего времени администратора ИБ. Также существует проблема, при которой администратор, не имея должного опыта в настройке СЗИ от НСД, может неверно настроить данное средство. Шаблонная настройка в этом плане более удобна. Основная проблема гибкой настройки с точки зрения информационной безопасности заключается в том, что администратор при наделении его чрезмерными полномочиями из-за личной выгоды может деструктивно повлиять на обеспечение безопасности данной информационной системы.

При проектировании подсистемы настройки средств защиты информации разработчик также может внедрить дополнительные функции настройки СЗИ от НСД. Данные функции предназначены для удобства использования с учетом особенностей информационных систем. Но иногда внедрение избыточных функций, может снизить обеспечиваемый уровень безопасности информации. В качестве иллюстрации данного утверждения можно привести реализацию одной из функций безопасности АПМДЗ «Соболь». Аппаратно-программный модуль доверенной загрузки позволяет осуществлять загрузку с диска, что

напрямую снижает обеспечиваемый уровень безопасности информации. Также разработчики программно-аппаратных комплексов для удовлетворения требований организаций, где в приоритете стоит доступность информации, могут разработать функцию, которая при блокировке или неисправности СЗИ способна экстренно отключить механизмы защиты. Данная функция напрямую снижает обеспечиваемый уровень безопасности информации, так как из программно-аппаратных механизмов защиты информации преобразует в программные механизмы.

Немаловажно при проектировании подсистемы настройки СЗИ от НСД, следует учитывать удобство пользовательского интерфейса. Администратор при настройке данного СЗИ может не разобраться с интерфейсом подсистемы и неверно настроить другие подсистемы, отвечающие за обеспечение безопасности информации. Также данная проблема может повлиять на трудоемкость настройки и оперативность работы с СЗИ от НСД.

3.3 Вывод

Из вышеизложенного можно сделать следующий вывод: проблемы безопасности, возникающие в результате настройки СЗИ от НСД, являются следствием того, что производитель стремится разработать СЗИ универсального применения. К данным проблемам можно отнести:

- Предоставление избыточных прав администратору ИБ, путем введения дополнительных функций;
- Сложный пользовательский интерфейс. Данная проблема может также стать следствием внедрения дополнительных функций. Администратор ИБ без должного опыта не сможет ориентироваться в настройках СЗИ.

Поэтому при проектировании подсистемы настройки СЗИ от НСД необходимо учитывать не только полноту функционала и удобство использования, но и отсутствие избыточных функций, использование которых

может снизить обеспечиваемый уровень безопасности информации. Для разработки подсистемы настройки СЗИ от НСД необходимо определить минимальное количество функций, требуемых для обеспечения безопасности в ИС. Требования к обеспечению безопасности в ИС, содержатся в отечественных нормативно-методических документах. Соответственно при разработке подсистемы настройки, необходимо из данных требований по обеспечению безопасности в ИС выявить требования реализуемые СЗИ от НСД.

4 Анализ технических требований по обеспечению информационной безопасности информационных систем, содержащихся в отечественных нормативно-методических документах

4.1 Объекты исследования

Для определения требований к подсистеме настройки СЗИ от НСД необходимо рассмотреть технические требования по обеспечению информационной безопасности в различных информационных системах, автоматизированных системах, а также требования к средствам вычислительной техники. Такие требования выдвигает ФСТЭК. Для получения более точного результата, необходимо рассмотреть большое количество требований. Согласно документу «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации» были определены требования необходимые для обеспечения информационной безопасности. В данном разделе рассматриваются:

- приказ ФСТЭК России от 11.02.2013 N 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
- приказ ФСТЭК России от 18.02.2013 N 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- приказ ФСТЭК России от 31.08.2010 N 489 «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования»;
- приказ ФСТЭК России от 14.03.2014 N 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных

системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»;

- руководящий документ ФСТЭК. Решение председателя Гостехкомиссии России от 30.03.1992 «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»;

- руководящий документ ФСТЭК. Решение председателя Гостехкомиссии России от 30.03.1992 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации»;

- методический документ ФСТЭК от 11.02.2014 «Меры защиты информации в государственных информационных системах».

Стоит отметить, что данных требований недостаточно, чтобы в полной мере СЗИ от НСД могло функционировать, так как данные требования ориентированы на функции администратора ИБ. В функции роли администратора ИБ СЗИ от НСД входят: обеспечение информационной безопасности в части защиты от несанкционированного доступа к ресурсам, включая контроль доступа к коммуникационным портам, АРМ и серверов подконтрольных СЗИ от НСД объектов. Соответственно есть дополнительные функции позволяющие администратору СЗИ от НСД производить установку ПО СЗИ от НСД и обеспечить общее функционирование КТС и ПО СЗИ от НСД. Требования, касающиеся администратора СЗИ от НСД в данном проекте не рассматриваются.

4.2 Исследование требований к различным типам информационных систем

Из данного массива требований необходимо выявить требования, относящиеся к различным типам информационных систем. К таким требованиями можно отнести:

- приказ ФСТЭК России от 11.02.2013 N 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
- приказ ФСТЭК России от 18.02.2013 N 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- приказ ФСТЭК России от 31.08.2010 N 489 «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования»;
- приказ ФСТЭК России от 14.03.2014 N 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».
- Целью данного раздела является выявление требований реализуемых средствами защиты информации. В целях экономии необходимо ввести условные обозначения требований, реализуемых СЗИ.

4.2.1 Идентификация и аутентификация

Первой группой требований является «Идентификация и аутентификация». К данной группе требований относятся следующие

требования: «идентификация и аутентификация пользователей, являющихся работниками оператора» (ИА1), «Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных» (ИА2); «Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов» (ИА3), «Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации» (ИА4), «Защита обратной связи при вводе аутентификационной информации» (ИА5), «Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)» (ИА6), «Идентификация и аутентификация объектов файловой системы, запускаемых и исполняемых модулей, объектов систем управления базами данных, объектов, создаваемых прикладным и специальным программным обеспечением, иных объектов доступа» (ИА7). Все требования данной группы реализуются непосредственно внутри СЗИ так как необходимы для определения и подтверждения субъекта внутри информационной системы.

4.3 Управление доступом субъектов доступа к объектам доступа

Следующей группой требований является «Управление доступом субъектов доступа к объектам доступа» [5, 6, 7, 8]. К данной группе требований относятся следующие требования: «Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей» (УД1). «Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа» (УД2), «Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами» (УД3), «Разделение полномочий (ролей)

пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы» (УД4), «Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы» (УД5), «Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)» (УД6), «Предупреждение пользователя при его входе в информационную систему о том, что в информационной системе реализованы меры защиты информации, и о необходимости соблюдения им установленных оператором правил обработки информации» (УД7), «Оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему» (УД8), «Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы» (УД9), «Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу» (УД10), «Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации» (УД11), «Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки» (УД12), «Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети» (УД13), «Регламентация и контроль использования в информационной системе технологий беспроводного доступа» (УД14), «Регламентация и контроль использования в информационной системе мобильных технических средств» (УД15), «Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)» (УД16), «Обеспечение доверенной загрузки средств вычислительной техники» (УД17). Требования данной группы реализуются непосредственно СЗИ так как данные функции необходимы для управления доступом субъекта к объектам внутри системы.

4.3.1 Ограничение программной среды

Следующая группа требований «Ограничение программной среды» [5, 6, 7, 8]. К ней относятся следующие требования: «Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения» (ОПС1); «Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения» (ОПС2) ; «Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов» (ОПС3); «Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов» (ОПС4) . Все требования данной группы выполняются при помощи СЗИ, так как средство защиты представляет собой совокупность инженерно-технических, электрических, электронных, оптических и других устройств и приспособлений, приборов и технических систем, а также иных вещных элементов, используемых для решения различных задач по защите информации, в том числе к данным средствам можно отнести программные и программно-аппаратные комплексы.

4.3.2 Защита машинных носителей информации

Следующая группа требований - «Защита машинных носителей информации» [5, 6, 7, 8]. Требование «Учет машинных носителей информации» - не выполняется СЗИ, так как это организационная мера реализуемая документированием машинных носителей. «Управление доступом к машинным носителям информации» данное требование не реализуется СЗИ, так как данная организационная мера реализуется ограничением физического доступа к

машинным носителям. «Контроль перемещения машинных носителей информации за пределы контролируемой зоны» - данное требование не реализуется СЗИ, так как реализуется организационными мерами по контролю за физическим перемещением машинных носителей. «Исключение возможности несанкционированного ознакомления с содержанием информации, хранящейся на машинных носителях, и (или) использования носителей информации в иных информационных системах» - данное требование не реализовано в СЗИ так как реализуется организационными мерами по физическому контролю машинных носителей. «Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации» (МН1) - данное требование реализуется внутри СЗИ, так как должен осуществляться контроль за портами внутри системы. «Контроль подключения машинных носителей информации» (МН2) - данное требование реализуется СЗИ, так как должны регулироваться подключаемые устройства внутри системы. «Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания)» - данное требование не реализуется в СЗИ, так как осуществляется организационными мерами посредством уничтожения информации.

4.3.3 Регистрация событий безопасности

Следующая группа требований «Регистрация событий безопасности» [5, 6, 7, 8]. Требования «Определение событий безопасности, подлежащих регистрации, и сроков их хранения» (РС1), «Определение состава и содержания информации о событиях безопасности, подлежащих регистрации» (РС2), «Сбор, запись и хранение информации о событиях безопасности в течении установленного времени хранения» (РС3), «Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или

переполнения объема (емкости) памяти» (РС4), «Генерирование временных меток и (или) синхронизация системного времени в информационной системе» (РС5), «Защита информации о событиях безопасности» (РС6), «Обеспечение возможности просмотра и анализа информации о действиях отдельных пользователей в информационной системе» (РС7) - реализуются внутри СЗИ, так как данные требования необходимы для осуществления мониторинга и выявления инцидентов информационной безопасности, а требование «Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них» - не выполняется СЗИ, так как относится к организационным мерам по анализу результатов регистрации событий .

4.3.4 Антивирусная защита

Требования группы «Антивирусная защита» [5, 6, 7, 8], такие как «Реализация антивирусной защиты» (А31), «Обновление базы данных признаков вредоносных компьютерных программ (вирусов)» (А32) выполняются СЗИ, так как к средствам защиты относятся антивирусные программы.

4.3.5 Обнаружение вторжений

Также группа требований «Обнаружение вторжений» [5, 6, 7, 8], куда входят такие требования как «Обнаружение вторжений» (ОВ1) и «Обновление базы решающих правил» (ОВ2) реализуются непосредственно СЗИ, так как данные требования выполняют системы обнаружения вторжений.

4.3.6 Контроль (анализ) защищенности информации

Далее рассматривается группа требований «Контроль (анализ) защищенности информации» [5, 6, 7, 8]. Требование «Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей» - не реализуется СЗИ, так как это организационная

мера. «Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации» - данное требование не реализуется внутри СЗИ, так как это организационная мера. «Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации» - не реализуется в СЗИ, так как это организационная мера возлагаемая на администратора информационной безопасности. «Контроль состава технических средств, программного обеспечения и средств защиты информации» - данное требование не реализуется в СЗИ, так как это организационная мера направленная на выявление и устранения недостатков СЗИ. «Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе» - требование не реализуется в СЗИ, так как это организационная мера.

4.3.7 Обеспечение целостности информационной системы и информации

Следующая группа требований «Обеспечение целостности информационной системы и информации» [5, 6, 7, 8].. Требования «Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации» (КЦ1) , «Контроль целостности информации, содержащейся в базах данных информационной системы» (КЦ2), «Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций» (КЦ3) , «Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама)» (КЦ4), «Контроль содержания информации, передаваемой из информационной системы (контейнерный, основанный на свойствах объекта доступа, и контентный, основанный на

поиске запрещенной к передаче информации с использованием сигнатур, масок и иных методов), и исключение неправомерной передачи информации из информационной системы» (КЦ5), «Ограничение прав пользователей по вводу информации в информационную систему» (КЦ6) , «Контроль точности, полноты и правильности данных, вводимых в информационную систему» (КЦ7) и «Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях» (КЦ8) выполняются в СЗИ, так как необходимо обеспечивать неизменность информационной системы и информации, от модификации и удаления.

4.3.8 Обеспечение доступности информации

Следующая группа требований «Обеспечение доступности информации» [5, 6, 7, 8]. Требование «Использование отказоустойчивых технических средств» не реализуется в СЗИ, так как это организационная мера направленная на выбор технических средств. «Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирования» не реализуется СЗИ, так как это организационная мера направленная на периодическую проверку работоспособности. «Периодическое резервное копирование информации на резервные машинные носители информации» - не реализуется СЗИ, так как это организационная мера, направленная на сохранение данных на резервных носителях. «Обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течении установленного временного интервала» – требование не реализуется СЗИ, так как это организационная мера. «Кластеризация информационной системы и (или) ее сегментов» - требование не реализуемое СЗИ, так как выделение групп однотипных узлов, объединенных каналами передачи информации и рассматриваемых как единый

программно-технический ресурс проходит без участия СЗИ. «Контроль состояния и качества предоставления уполномоченным лицом вычислительных ресурсов (мощностей), в том числе по передаче информации» - требование не реализуемое СЗИ, так как это организационная мера направленная на мониторинг оператором состояния ресурсов.

4.3.9 Защита среды виртуализации

Группа требований «Защита среды виртуализации» [5, 6, 7, 8]. Такие требования как : «Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации» (CB1), «Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин» (CB2) , «Регистрация событий безопасности в виртуальной инфраструктуре» (CB3), «Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры» (CB4) , «Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией» (CB5) , «Контроль целостности виртуальной инфраструктуры и ее конфигураций» (CB6), «Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры» (CB7), «Реализация и управление антивирусной защитой в виртуальной инфраструктуре» (CB8), «Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей» (CB9) - реализуются в СЗИ, и выполняется средствами защиты информации среды виртуализации. «Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных» - не реализуются, так как это организационная

мера, направленная на контроль физического перемещения виртуальных машин.

4.3.10 Защита технических средств

Следующая группа требований «Защита технических средств» [5, 6, 7, 8]. Требование «Защита информации, обрабатываемой техническими средствами, от ее утечки по техническим каналам» (ЗТС1) - реализуется техническими СЗИ по утечке акустическим, электромагнитным и других видов технических каналов, которые. «Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования» требование не реализуемое СЗИ, так как это организационная мера направленная на контроль физического перемещения. «Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены» - требования не реализуемые СЗИ, так как это организационная мера направленная на контроль физического доступа. «Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр»- требование не реализуемое СЗИ, так как это организационная мера. «Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов)» - требование не реализуемое СЗИ, так как это организационная мера. [5]

4.3.11 Защита информационной системы, ее средств, систем связи и передачи данных

Группа требований «Защита информационной системы, ее средств, систем связи и передачи данных» [5, 6, 7, 8]. К данной группе требований относятся такие требования как: «Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации, функций по обработке информации и иных функций информационной системы» (ЗИС1) - требование реализуемое СЗИ, так как это организационная мера. «Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом» (ЗИС2) - требование реализуемое СЗИ. «Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи» (ЗИС3) - требование реализуемое средствами криптографической ЗИ, так как необходимо обеспечить безопасность передачи по каналам связи. «Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации)» (ЗИС4) - требование реализуемое средствами криптографической ЗИ, так как необходимо реализовать безопасность канала передачи данных . «Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств» (ЗИС5) - требование реализуемое средствами криптографической ЗИ «Передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с информацией, при обмене информацией с иными информационными системами» (ЗИС6) - требование реализуемое СЗИ, так как

необходимо обеспечить безопасность информации от ее модификации или удаления. «Контроль санкционированного и исключение несанкционированного использования технологий передачи речи, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи» (ЗИС7) - требование реализуемое СКЗИ, так как необходимо обеспечить безопасность речевой информации передаваемой по каналам связи. «Контроль санкционированной и исключение несанкционированной передачи видеоинформации, в том числе регистрация событий, связанных с передачей видеоинформации, их анализ и реагирование на нарушения, связанные с передачей видеоинформации» (ЗИС8) - требование реализуемое СЗИ, так как необходимо обеспечить безопасность информации и регистрацию событий. «Подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам» (ЗИС9) – требование реализуемое СЗИ. «Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов» (ЗИС10) – требование реализуемое СЗИ, так как необходимо определить. «Исключение возможности отрицания пользователем факта отправки информации другому пользователю» (ЗИС11) - требование реализуемое СЗИ, осуществляемое регистрацией событий.. «Использование устройств терминального доступа для обработки информации» (ЗИС12) - требование реализуемое СЗИ. «Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации» (ЗИС13) - требование реализуемое СЗИ. «Выявление, анализ и блокирование в информационной системе скрытых каналов передачи информации в обход реализованных мер защиты информации или внутри разрешенных сетевых протоколов» - требование не реализуемое СЗИ, так как это организационная

мера направленная на выявление оператором скрытых каналов связи. «Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы» (ЗИС14) - требование реализуемое СЗИ, при котором создается многоуровневая система безопасности. «Обеспечение загрузки и исполнения программного обеспечения с машинных носителей информации, доступных только для чтения, и контроль целостности данного программного обеспечения» (ЗИС15) требование реализуемое СЗИ при котором должен осуществляться контроль машинных носителей. «Изоляция процессов (выполнение программ) в выделенной области памяти» (ЗИС16) - требование реализуемое СЗИ, так как должна обеспечиваться недоступность областей памяти используемых одним пользователем, для процессов другого пользователя. «Защита беспроводных соединений, применяемых в информационной системе» (ЗИС17) - требование реализуемое СЗИ, обеспечивающее безопасность информации по средством криптографической защиты. «Исключение доступа пользователя к информации, возникшей в результате действий предыдущего пользователя через реестры, оперативную память, внешние запоминающие устройства и иные общие для пользователей ресурсы информационной системы» (ЗИС18) - требование реализуемое СЗИ. «Защита информационной системы от угроз безопасности информации, направленных на отказ в обслуживании информационной системы» (ЗИС19) требование реализуемое СЗИ, так как необходимо обнаружить атаки направленные на отказ в обслуживании. «Защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями» - требование не реализуемое СЗИ, так как обеспечивается организационной мерой контроль физических границ. «Прекращение сетевых соединений по их завершении или по истечении заданного оператором временного интервала неактивности сетевого

соединения» - требование не реализуемого в СЗИ, так как это реализуется заданным интервалом времени по отключению порта/адреса и прекращению сетевых соединений. «Использование в информационной системе или ее сегментах различных типов общесистемного, прикладного и специального программного обеспечения (создание гетерогенной среды)» - требование не реализуемое в СЗИ, так как реализуется проектировщиками ИС. «Использование прикладного и специального программного обеспечения, имеющих возможность функционирования в средах различных операционных систем» - требование не реализуемое в СЗИ, так как это организационная мера направленная на выбор и использования программного обеспечения, для обеспечения безопасности при атаках. «Создание (эмуляция) ложных информационных систем или их компонентов, предназначенных для обнаружения, регистрации и анализа действий нарушителей в процессе реализации угроз безопасности информации» требование не реализуемое в СЗИ, так как создаются проектировщиком ИС «Воспроизведение ложных и (или) скрывание истинных отдельных информационных технологий и (или) структурно-функциональных характеристик информационной системы или ее сегментов, обеспечивающее навязывание нарушителю ложного представления об истинных информационных технологиях и (или) структурно-функциональных характеристиках информационной системы» требование не реализуемое СЗИ. «Перевод информационной системы или ее устройств (компонентов) в заранее определенную конфигурацию, обеспечивающую защиту информации, в случае возникновения отказов (сбоев) в системе защиты информации информационной системы» (ЗИС20) - требование реализуемое СЗИ, так как в случае сбоев или отказов информационная система должна быть переведена в конфигурацию обеспечивающую защиту информации. «Защита мобильных технических средств, применяемых в информационной системе» (ЗИС21) - требование реализуемое СЗИ, так как внутри ИС необходимо контролировать съемные носители, жесткие диски, флэш-накопители и.т.д.[5]

4.3.12 Другие группы требований к ИС

Группы требований такие как: «Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ)», «Контроль (анализ) защищенности персональных данных (АНЗ)», «Управление конфигурацией автоматизированной системы управления и ее системы защиты (УКФ)», «Выявление инцидентов и реагирование на них (ИНЦ)», «Анализ угроз безопасности информации рисков от их реализации (УБИ)», «Информирование и обучение персонала (ИПО)», «Обеспечение действий в нештатных (непредвиденных) ситуациях (ДНС)», «Планирование мероприятий по обеспечению защиты информации (ПЛН)», «Управление обновлениями программного обеспечения (ОПО)», «Обеспечение безопасной разработки программного обеспечения» содержат организационные меры, соответственно в данном проекте не рассматриваются. [8]

4.4 Исследование требований к автоматизированным системам

В данном разделе рассматриваются требования к АС. Данные требования регулируются в руководящем документе «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации».

К подсистеме управления доступом относятся следующие требования:

«Идентификация, проверка подлинности и контроль доступа субъектов:

- в систему;
- к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним;
- устройствам ЭВМ;
- к программам;
- к томам, каталогам, файлам, записям, полям записей.» (АС1);

– Данное требование реализуется в СЗИ, так как так как необходимы для определения и подтверждения субъекта внутри системы, «Управление потоками информации» (АС2) данное требование реализуется в СЗИ, так как данная функция необходима для управления доступом субъекта к объектам внутри системы

Группа требований применимая к подсистеме регистрации и учета

«Регистрация и учет:

- входа (выхода) субъектов доступа в (из) систему(ы) (узел сети);
- выдачи печатных (графических) выходных документов;
- запуска (завершения) программ и процессов (заданий, задач);
- доступа программ субъектов доступа к защищаемым файлам,
- включая их создание и удаление, передачу по линиям и каналам связи;
- доступа программ субъектов доступа к терминалам, ЭВМ, узлам;
- сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей;
- изменения полномочий субъектов доступа;
- создаваемых защищаемых объектов доступа» (АС3) - данные требования реализуются в СЗИ, так как необходимо вести учет всех инцидентов для последующего реагирования.

«Учет носителей информации» (АС4) - данное требование не реализуется в СЗИ, так как это организационная мера. «Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей» (АС5) данное требование реализуется в СЗИ, «Сигнализация попыток нарушения защиты» (АС6) - реализуется в СЗИ, так как необходима немелкая реакция на инцидент информационной Безопасности.

Группа требований применимая к криптографической подсистеме. «Шифрование конфиденциальной информации» (АС7) - требование реализуется в СЗИ, это необходимо для обеспечения безопасности. «Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах» (АС8) требование реализуется в СЗИ, так как это необходимо для обеспечения безопасности информации. «Использование аттестованных (сертифицированных) криптографических средств» требование не реализуется в СЗИ, это организационная мера направленная на выбор СЗИ.

Группа требований применимая к подсистеме обеспечения целостности. «Обеспечение целостности программных средств и обрабатываемой информации» (АС9) - требование реализуемое в СЗИ, так как необходимо обеспечить неизменность информации и программных средств. «Физическая охрана средств вычислительной техники и носителей информации» - требование не реализуемое в СЗИ, так как это организационная мера, направленная на физический контроль СВТ и носителей информации «Наличие администратора (службы) защиты информации в АС» - требование не реализуемое в СЗИ, так как это организационная мера. «Периодическое тестирование СЗИ НСД» - требование не реализуемое в СЗИ, так как это организационная мера направленная на проверку работоспособности. «Наличие средств восстановления СЗИ НСД» (АС10) - требование реализуемое в СЗИ, так как при сбое необходимо в кратчайшие сроки восстановить работоспособность. «Использование сертифицированных средств защиты» требование не реализуемое в СЗИ, так как это организационная мера направленная на выбор средства защиты информации [9].

4.5 Исследование требований к средствам вычислительной техники

В данном разделе рассматриваются требования к СВТ. Данные требования регулируются в документе «Средства вычислительной техники.

Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации».

Требование «Дискреционный принцип контроля доступа» (СВТ1) - реализуется непосредственно в СЗИ, так как это один из способов разграничения доступа «Мандатный принцип контроля доступа» (СВТ2) - реализуется в СЗИ, так как это один из способов разграничения доступа «Очистка памяти» (СВТ3) - требование реализуется в СЗИ, так как необходима очистка оперативной памяти. «Изоляция модулей» (СВТ4) - реализуется в СЗИ, так как необходимо изолировать область памяти одного субъекта, от области памяти другого субъекта «Маркировка документов» (СВТ5) - требование реализуемое в СЗИ. «Защита ввода и вывода на отчуждаемый физический носитель информации» (СВТ6) - требование реализуемое СЗИ, так как необходим контроль за каналами «Сопоставление пользователя с устройством» (СВТ7) - требование реализуемое СЗИ. «Идентификация и аутентификация» (СВТ8) - требование реализуемое в СЗИ, необходимо для определения доступа субъекта к объекту. «Гарантии проектирования» требование не реализуемое СЗИ, должна быть осуществлена модель доступа «Регистрация» (СВТ9) - требование реализуемое СЗИ, необходимая для обнаружения инцидентов ИБ. «Взаимодействие пользователя с КСЗ» (СВТ10) - требование реализуемое СЗИ. «Надежное восстановление» (СВТ11) - требование реализуемое СЗИ, в случае сбоя необходимо восстановление «Целостность КСЗ» (СВТ12) - требование реализуемое СЗИ, так как необходимо для контроля неизменности КСЗ. «Контроль модификации» - требование не реализуемое СЗИ. «Контроль дистрибуции» - требование не реализуемое в СЗИ, так как должно быть проверенно соответствие документации и текста программ «Гарантии архитектуры» (СВТ13) - требование реализуемое в СЗИ, и регулируется перехватом всех сообщений субъекта к объектам. «Тестирование» - требование не реализуемое в СЗИ, так как это организационная мера направленная на проверку работоспособности.

Требования: «Руководство для пользователя», «Руководство по КСЗ», «Тестовая документация», «Конструкторская (проектная) документация» - с технической точки зрения в СЗИ не реализуется, так как это документация. [10]

4.6 Вывод

Из данного раздела можно сделать вывод, что основное количество требований реализуется средствами защиты информации. Остальные же требования заключались больше в обеспечении организационных мер. Данный анализ позволил выбрать требования, реализуемые техническими средствами. Но так как существует множество видов СЗИ, например средства обнаружения вторжений, антивирус и т. д., а в данном проекте рассматривается разработка подсистемы настройки СЗИ от НСД, то существует необходимость в первую очередь определить требования к СЗИ от НСД.

5 Классификация технических требований в зависимости от степени и характера влияния на компоненты подсистемы настройки средств защиты информации от несанкционированного доступа

5.1 Требования к средствам защиты информации от несанкционированного доступа

После анализа технических требований, необходимо определить требования реализуемые посредством СЗИ от НСД. Сначала рассматриваются требования применимые к информационным системам.

Первой группой требований является «Идентификация и аутентификация». К данной группе требований относятся следующие требования: «ИА1», «ИА2», «ИА3», «ИА4», «ИА5», «ИА6», «ИА7». Все требования данной группы реализуются непосредственно внутри СЗИ от НСД, так как это одна из основных функций предоставления доступа субъекта к объекту.

Следующей группой требований является «Управление доступом субъектов доступа к объектам доступа». К данной группе требований относятся следующие требования: «УД1», «УД2», «УД3», «УД4», «УД5», «УД6», «УД7», «УД8», «УД9», «УД10», «УД11», «УД12», «УД13», «УД14», «УД15», «УД16», «УД17». Требования данной группы реализуются непосредственно СЗИ от НСД, так как они необходимы для разграничения доступа субъекта к объектам.

Следующая группа требований «Ограничение программной среды». К ней относятся следующие требования: «ОПС1», «ОПС2», «ОПС3», «ОПС4». Все требования данной группы выполняются про помощи СЗИ от НСД, так как СЗИ от НСД классифицируются как программные и программно-аппаратные комплексы.

Следующая группа требований - «Защита машинных носителей информации». «МН1» - данное требование реализуется внутри СЗИ от НСД, так как необходим контроль портов, как средства ввода-вывода информации. «МН2» - данное требование реализуется СЗИ о НСД, так как должны регулироваться подключаемые устройства внутри системы.

Следующая группа требований «Регистрация событий безопасности». Требования «РС1», «РС2», «РС3», «РС4», «РС5», «РС6», «РС7» - реализуются внутри СЗИ от НСД, так как инциденты информационной безопасности должны фиксироваться.

Требования группы «Антивирусная защита», такие как реализация антивирусной защиты «А31» и обновление базы данных признаков вредоносных компьютерных программ «А32» не выполняются в СЗИ от НСД, так как выполняются Антивирусными программами.

Также группа требований «Обнаружение вторжений», куда входят такие требования как обнаружение вторжений «ОВ1» и обновление базы решающих правил «ОВ2» не реализуются в СЗИ от НСД, так как выполняются Средствами обнаружения вторжений

Следующая группа требований «Обеспечение целостности информационной системы и информации». Требования как: «КЦ1», «КЦ2», «КЦ3», «КЦ4», «КЦ5», «КЦ6», «КЦ7», «КЦ8» - выполняются в СЗИ от НСД, так как необходимо обеспечивать неизменность информационной системы и информации, в частности при несанкционированном доступе.

Группа требований «Защита среды виртуализации». Такие требования как : «СВ1», «СВ2», «СВ3», «СВ4», «СВ5», «СВ6», «СВ7», «СВ9» - реализуется в СЗИ от НСД, так как необходимо обеспечить защиту информации при использовании среды виртуализации а требование реализации и управлении антивирусной защитой в виртуальной инфраструктуре «СВ8» - не реализуется в СЗИ от НСД., так как это реализует антивирусная программа

Следующая группа требований «Защита технических средств». Требование защита информации, обрабатываемой техническими средствами, от ее утечки по техническим каналам «ЗТС1» - не реализуется СЗИ от НСД, так как данное требование реализуется техническими средствами защиты информации(использование экранированного кабеля, контролируемых зон итд).

Группа требований «Защита информационной системы, ее средств, систем связи и передачи данных». К данной группе относятся следующие требования: «ЗИС6», «ЗИС7», «ЗИС9», «ЗИС11», «ЗИС12», «ЗИС18», «ЗИС19», «ЗИС21» - Данные требования реализуются СЗИ от НСД, а требования «ЗИС1», «ЗИС2», «ЗИС3», «ЗИС4», «ЗИС5», «ЗИС8», «ЗИС10», «ЗИС13», «ЗИС14», «ЗИС15», «ЗИС16», «ЗИС17» и «ЗИС20» - не реализуются СЗИ от НСД, так как реализуются СКЗИ или иными СЗИ.

Теперь рассматриваются требования к АС реализуемые в СЗИ. К данным требованиям относятся : «АС1», «АС2», «АС3», «АС4», «АС5», «АС6», «АС7», «АС8», «АС9», «АС10». Все приведенные требования реализуются в СЗИ от НСД.

Далее необходимо рассмотреть требования к СВТ реализуемые СЗИ. К данным требованиям относятся: «СВТ1», «СВТ2», «СВТ3», «СВТ4», «СВТ5», «СВТ6», «СВТ8», «СВТ9», «СВТ11», «СВТ12», «СВТ13» - данные требования реализуются СЗИ от НСД. А сопоставление пользователя с устройством «СВТ7» и взаимодействие пользователя с КСЗ «СВТ10» – не реализуются СЗИ от НСД.

5.2 Высокоуровневые требования к подсистеме настройки средств защиты информации от несанкционированного доступа

После анализа технических требований реализуемых посредством СЗИ от НСД, необходимо определить требования, нуждающиеся в настройке внутри

СЗИ от НСД. Сначала рассматриваются требования применимые к информационным системам.

Первой группой требований является «Идентификация и аутентификация». К данной группе требований относятся следующие требования: «ИА1», «ИА3», «ИА4» - Нуждаются в настройке внутри СЗИ от НСД. А требования «ИА2», «ИА4», «ИА5», «ИА6», «ИА7» - не нуждается в настройке, так как реализовано внутри СЗИ от НСД

Следующей группой требований является «Управление доступом субъектов доступа к объектам доступа». К данной группе требований относятся следующие требования: «УД1», «УД2», «УД4», «УД5», «УД6» «УД10», «УД11», «УД12», «УД14», «УД17» - данные требования нуждаются в настройке внутри СЗИ от НСД. «УД3», «УД7», «УД8», «УД9», «УД13», «УД15», «УД16» - данные требования не нуждаются в настройке так как реализованы внутри СЗИ от НСД

Следующая группа требований «Ограничение программной среды». К ней относятся следующие требования: «ОПС1», «ОПС2» - нуждаются в настройке внутри СЗИ от НСД. А требования «ОПС3» и «ОПС4» не нуждается в настройке так как реализованы внутри СЗИ от НСД.

Следующая группа требований - «Защита машинных носителей информации». Требования «МН1» и «МН2» - нуждаются в настройке внутри СЗИ от НСД

Следующая группа требований «Регистрация событий безопасности». Требования «РС1», «РС2» - нуждаются в настройке внутри СЗИ от НСД. А требования «РС3», «РС4», «РС5», «РС6», «РС7» - не нуждается в настройке так как реализованы внутри СЗИ от НСД

Следующая группа требований «Обеспечение целостности информационной системы и информации». Требования «КЦ1» «КЦ2» «КЦ6» - нуждаются в настройке в нутрии СЗИ от НСД, а требования «КЦ3», «КЦ4»,

«КЦ5», «КЦ7», «КЦ8» - не нуждающиеся в настройке, так как реализованы внутри СЗИ от НСД.

Группа требований «Защита среды виртуализации». Такие требования как : «СВ1», «СВ2», «СВ3», «СВ4», «СВ5», «СВ6», «СВ7», «СВ9» - данные требования нуждаются в настройке внутри СЗИ от НСД, но так как данные требования реализованы в предыдущих группах требований они не учитываются.

Следующая группа требований «Защита информационной системы, ее средств, систем связи и передачи данных». К ней относятся такие требования как: «ЗИС6», «ЗИС7», «ЗИС9», «ЗИС11», «ЗИС12», «ЗИС18», «ЗИС19», «ЗИС21» -данные требования не нуждаются в настройке, так как реализованы внутри СЗИ от НСД.

Теперь рассматриваются требования к АС реализуемые СЗИ от НСД, такие как : «АС1», «АС3», «АС9» - нуждаются в настройке внутри СЗИ от НСД , а требования «АС2», «АС5», «АС6», «АС7», «АС8», «АС10» - не нуждаются в настройке внутри СЗИ от НСД.

Далее необходимо рассмотреть требования к СВТ реализуемые в СЗИ от НСД. «СВТ1», «СВТ2», «СВТ6», «СВТ8», «СВТ9», «СВТ12», - данные требования необходимы в настройке внутри СЗИ от НСД.. Требования «СВТ3», «СВТ4», «СВТ5», «СВТ11», «СВТ13» - данные требования не нуждаются в настройке, так как реализованы внутри СЗИ от НСД.

5.3 Номенклатура компонентов подсистемы настройки средства защиты информации от несанкционированного доступа

На основе результатов разработки требований можно определить состав компонентов подсистемы настройки СЗИ от НСД. К таким компонентам относятся:

- идентификация и аутентификация;

- управление доступом;
- ЗПС;
- управление носителями информации;
- регистрация и учет;
- КЦ.

Результаты классификации требований реализуемых конфигурациями СЗИ от НСД представлены в сводной таблице 1.

Таблица 1 – Классификация требований реализуемых конфигурацией СЗИ от НСД

Компонент подсистемы настройки СЗИ от НСД	Требования к ИС	Требования к АС	Требования к СВТ
Идентификация и аутентификация	« ИА1» Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных	«АС1» Идентификация, проверка подлинности и контроль доступа субъектов: в систему к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ к программам	«СВТ8» Идентификация и аутентификация
	«ИА3» Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов		

Продолжение таблицы 1 - Классификация требований реализуемых конфигурациями СЗИ от НСД

Компонент подсистемы настройки СЗИ от НСД	Требования к ИС	Требования к АС	Требования к СВТ
	«ИА3» Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	к томам, каталогам, файлам, записям, полям записей	
Управление доступом	«УД1» Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей		

Продолжение таблицы 1 - Классификация требований реализуемых конфигурациями СЗИ от НСД

Компонент подсистемы настройки СЗИ от НСД	Требования к ИС	Требования к АС	Требования к СВТ
	«УД2» Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа		«СВТ1» Дискреционный принцип контроля доступа; «СВТ2» Мандатный принцип контроля доступа.
	«УД4» Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы		
	«УД5» Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы		
	«УД6» Ограничение		

Продолжение таблицы 1 - Классификация требований реализуемых конфигурациями СЗИ от НСД

Компонент подсистемы настройки СЗИ от НСД	Требования к ИС	Требования к АС	Требования к СВТ
	неуспешных попыток входа в информационную систему (доступа к информационной системе)		
	«УД10» Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу		
	«УД11» Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации		
	«УД12» Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки		

Продолжение таблицы 1 - Классификация требований реализуемых конфигурациями СЗИ от НСД

Компонент подсистемы настройки СЗИ от НСД	Требования к ИС	Требования к АС	Требования к СВТ
	«УД14» Регламентация и контроль использования в информационной системе мобильных технических средств		
	«УД17» Обеспечение доверенной загрузки средств вычислительной техники		
Замкнутая программная среда	«ОПС1» Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения		

Продолжение таблицы 1 - Классификация требований реализуемых конфигурациями СЗИ от НСД

Компонент подсистемы настройки СЗИ от НСД	Требования к ИС	Требования к АС	Требования к СВТ
	«ОПС2» Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения		
Управление носителями информации	«МН1» Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации		«СВТ6» Защита ввода и вывода на отчуждаемый физический носитель информации
	«МН2» Контроль подключения машинных носителей информации		
Регистрация и учет	«РС1» Определение событий безопасности, подлежащих	«АС3» Регистрация и учет: входа (выхода) субъектов	«СВТ9» Регистрация

Продолжение таблицы 1 - Классификация требований реализуемых конфигурациями СЗИ от НСД

Компонент подсистемы настройки СЗИ от НСД	Требования к ИС	Требования к АС	Требования к СВТ
	регистрации, и сроков их хранения	доступа в (из) систему(ы) (узел сети)	
	«РС2» Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	выдачи печатных (графических) выходных документов запуска (завершения) программ и процессов (заданий, задач) доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей	

Продолжение таблицы 1 - Классификация требований реализуемых конфигурациями СЗИ от НСД

Компонент подсистемы настройки СЗИ от НСД	Требования к ИС	Требования к АС	Требования к СВТ
		изменения полномочий субъектов доступа создаваемых защищаемых объектов доступа»	
Контроль целостности	«КЦ1» Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации	«АС9» Обеспечение целостности программных средств и обрабатываемой информации	«СВТ12» Целостность КСЗ
	«КЦ2» Контроль целостности информации, содержащейся в базах данных информационной системы		
	«КЦ6» Ограничение прав пользователей по вводу		

Продолжение таблицы 1 - Классификация требований реализуемых конфигурациями СЗИ от НСД

Компонент подсистемы настройки СЗИ от НСД	Требования к ИС	Требования к АС	Требования к СВТ
	информации в информационную систему		

5.4 Вывод

Не смотря на большое количество рассматриваемых нормативно-методических документов по обеспечению информационной безопасности, все они имеют схожие концепции в обеспечении технической защиты информации. Также исходя из таблицы 1 можно определить список компонентов составляющих подсистему настройки СЗИ от НСД. Стоит отметить, что данных функций не достаточно для обеспечения работоспособности системы. Поэтому данные требования необходимы только для обеспечения информационной безопасности в защите от несанкционированного доступа к ресурсам. Требования по обеспечению общего функционирования СЗИ от НСД в данном проекте не рассматриваются

6 Формирование комплекса требований к подсистеме настройки средств защиты информации от несанкционированного доступа

6.1 Требования по защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах

Для формирования комплекса требований к подсистеме настройки СЗИ от НСД на основе результатов приведенных в таблице 1 необходимо сформулировать низкоуровневые требования. Так как высокоуровневые требования к подсистеме настройки СЗИ от НСД из разных источников совпадают, а наиболее подробно они описаны в нормативно-методическом документе ФСТЭК от 11 февраля 2014 «Меры защиты информации в государственных информационных системах», то требования к реализации, на основе которых будут разработаны требования взяты из данного документа.

Согласно требованиям к реализации «ИА1» подсистема настройки идентификации и аутентификации нуждается в формировании идентификатора пользователя или устройства. Также необходимо реализовать исключение повторного использования идентификатора (не менее одного года, не менее трех лет, в течение всего периода эксплуатации). Необходимо блокировать идентификатор пользователя через период времени неиспользования и управлять идентификаторами внешних пользователей. [12]

Согласно требованиям к реализации «ИА3» необходимо по создавать и изменять аутентификационную информацию, также вносить изменения характеристик пароля, где задаются значения длины пароля (не менее 6 символов) , алфавит пароля (не менее 30 символов), количество неуспешных попыток аутентификации(выбор значений в поле от 3 до 10 попыток), а также установки времени блокировки в случае неуспешного ввода (от 3 до 60 минут) и промежутков времени на смену пароля (не более 180 дней) . [12]

Согласно требованиям к реализации «МН1» необходимо определять тип учетной записи (внутренний пользователь, внешний пользователь, гость, временная учетная запись и предоставить возможность создавать свои типы пользователей), заведение, активация, блокирование и уничтожение учетных записей пользователей, корректировки учетных записей автоматическое удаление временных учетных записей, для определения срока актуальности учетной записи, по автоматическое блокирование неиспользуемых учетных записей (более 90 дней, более 45 дней), блокирование учетных записей.

Согласно требованиям к реализации «УД2» необходимо реализовать мандатное и дискреционное разграничение доступа. [12]

Согласно требованиям к реализации «УД4» необходимо реализовать разграничение ролей (один пользователь может обладать только одной ролью) . [12]

Согласно требованиям к реализации «УД5» необходимо реализовать предоставление операторам прав к функциям безопасности, также запрет привилегий внешним пользователям. [12]

Согласно требованиям к реализации «УД6» необходимо реализовать ограничение неуспешных попыток входа в информационную систему, а также возможность разблокировки учетной записи. [12]

Согласно требованиям к реализации «УД10» необходимо определять время бездействия пользователя (до 15 минут) По истечении времени происходит завершение сеанса пользователя(выход из системы) . [12]

Согласно требованиям к реализации «УД11» необходимо реализовать выбор количества действий разрешенных до идентификации и аутентификации. [12]

Согласно требованиям к реализации «УД12» необходимо реализовать по обновление, назначение, изменение и сохранение атрибутов безопасности (меток безопасности) . [12]

Согласно требованиям к реализации «УД14» необходимо обеспечить контроль и регламентацию съемных носителей. [12]

Согласно требованиям к реализации «УД17» должны определяться компоненты доверенной загрузки. [12]

Согласно требованиям к реализации «ОПС1» необходимо обеспечить определение перечня компонентов программного обеспечения запускаемых автоматически при загрузке операционной системы, а также реализовано управление временем запуска и завершения работы компонентов программного обеспечения. [12]

Согласно требованиям к реализации «ОПС2» должно быть определение перечня компонентов программного обеспечения запускаемых автоматически при загрузке операционной системы. [12]

Согласно требованиям к реализации «МН1» в ИС должно быть обеспечение контроля интерфейсов ввода-вывода, регистрация, отключение. [12]

Согласно требованиям к реализации «МН2» должен осуществляться контроль машинных носителей разрешенные или запрещенные типы носителей, или же конкретные носители. [12]

Согласно требованиям к реализации «РС1» должен определяться тип событий подлежащих регистрации, а также тип данных хранимой информации. А именно о событиях безопасности, всех записей журналов итд. Также определение хранения файлов, журналов, или записей. [12]

Согласно требованиям к реализации «РС2» необходимо определять состав и содержание информации о событиях безопасности. [12]

Согласно требованиям к реализации «КЦ2» необходимо реализовать установку периодичности контроля целостности базы данных, а также выбор баз данных для контроля целостности, выбор модулей баз данных. [12]

Согласно требованиям к реализации «КЦб» необходимо осуществить ограничение прав пользователей по вводу информации в ИС. Реализовать выбор объектов файловой системы, объектов баз данных, объектов прикладного и специального программного обеспечения. [12]

6.2 Низкоуровневые требования к подсистеме настройки средств защиты информации от несанкционированного доступа

На основе требований к реализации приведенных в разделе 6, необходимо определить низкоуровневые требования к подсистеме настройки СЗИ от НСД.

Результаты формирования требований к подсистеме настройки идентификации и аутентификации представлены в таблице 2.

Результаты формирования требований к подсистеме настройки управления доступом представлены в таблице 3.

Результаты формирования требований к подсистеме настройки ЗПС представлены в таблице 4.

Результаты формирования требований к подсистеме управления носителями информации представлены в таблице 5.

Результаты формирования требований к подсистеме регистрации и учета представлены в таблице 6.

Результаты формирования требований к подсистеме контроля целостности представлены в таблице 7.

Продолжение таблицы 2 - Требования к подсистеме настройки идентификации и аутентификации

Требования к подсистеме идентификации и аутентификации	Низкоуровневые требования
Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	Реализовать функцию, где формируется идентификатор пользователя или устройства.

Продолжение таблицы 2 - Требования к подсистеме настройки идентификации и аутентификации

Требования к подсистеме идентификации и аутентификации	Низкоуровневые требования
	<p>Реализовать функцию исключающую повторное использование идентификатора и задать значения :</p> <p>а) не менее одного года;</p> <p>б) не менее трех лет;</p> <p>в) в течение всего периода эксплуатации информационной системы;</p>
	<p>Реализовать функцию, блокирующую идентификатор пользователя через период времени неиспользования, в котором можно задать значения:</p> <p>а) не более 90 дней;</p> <p>б) не более 45 дней;</p>
	<p>Реализовать функцию, в которой обеспечивается управление идентификаторами внешних пользователей.</p>
<p>Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации</p>	<p>Реализовать функцию по созданию и изменению аутентификационной информации</p>
	<p>Реализовать функцию изменения характеристик пароля, где задаются значения длины пароля (не менее 6 символов) , алфавит пароля (не менее 30 символов), количество неуспешных попыток аутентификации(выбор значений в поле от 3до 10 попыток), а также</p>

Продолжение таблицы 2 - Требования к подсистеме настройки идентификации и аутентификации

Требования к подсистеме идентификации и аутентификации	Низкоуровневые требования
	установки времени блокировки в случае неуспешного ввода (от 3 до 60 минут) и промежуток времени на смену пароля (не более 180 дней).

Продолжение таблицы 3 - Требования к подсистеме настройки управления доступом

Требования к подсистеме управления доступом	Низкоуровневые требования
Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	Реализовать функцию, где определяется тип учетной записи (внутренний пользователь, внешний пользователь, гость, временная учетная запись и предоставить возможность создавать свои типы пользователей)
	Реализовать функцию группирования учетных записей
	Реализовать функцию заведения, активации, блокирования и уничтожения учетных записей пользователей.
	Реализовать функцию корректировки учетных записей
	Реализовать функцию автоматического удаления временных учетных записей, для определения срока актуальности учетной записи

Продолжение таблицы 3 - Требования к подсистеме настройки управления доступом

Требования к подсистеме управления доступом	Низкоуровневые требования
	<p>Реализовать функцию по автоматическому блокированию неиспользуемых учетных записей, с временными значениями</p> <p>а) более 90 дней;</p> <p>б) более 45 дней;</p>
	<p>Реализовать функцию блокирования учетных записей :</p> <p>а) при превышении установленного оператором числа неуспешных попыток аутентификации пользователя.</p> <p>б) при выявлении по результатам мониторинга журналов регистрации событий безопасности действий пользователей, которые отнесены оператором к событиям нарушения безопасности информации.</p>
<p>Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа</p>	<p>Реализовать настройку дискреционного метода разграничения</p>
	<p>Реализовать настройку мандатного метода разграничения</p>
<p>Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы</p>	<p>В подсистеме настройки необходимо реализовать функцию разграничения ролей один пользователь может обладать только одной ролью.</p>
<p>Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы</p>	<p>В подсистеме настройки необходимо реализовать функцию по предоставлению операторам прав к функциям безопасность, также запрет привилегий</p>

Продолжение таблицы 3 - Требования к подсистеме настройки управления доступом

Требования к подсистеме управления доступом	Низкоуровневые требования
	внешним пользователям.
Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)	Реализовать функцию по ограничению неуспешных попыток входа в информационную систему, где задается максимальное количество попыток.
	Реализовать функцию разблокировки учетной записи.
Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу	В подсистеме настройки необходимо реализовать функцию определяющую время бездействия пользователя: а) до 15 минут; б) до 5 минут; По истечении времени происходит завершение сеанса пользователя(выход из системы)
Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации	В подсистеме настройки необходимо реализовать функцию по выбору количества действий разрешенных до идентификации и аутентификации.
Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки	В подсистеме настройки необходимо реализовать функцию по обновлению, назначению, изменению и сохранению атрибутов безопасности (меток безопасности)
Регламентация и контроль использования в информационной системе мобильных технических средств	В подсистеме настройки необходимо реализовать контроль и регламентацию съемных носителей

Продолжение таблицы 3 - Требования к подсистеме настройки управления доступом

Требования к подсистеме управления доступом	Низкоуровневые требования
Обеспечение доверенной загрузки средств вычислительной техники	В подсистеме настройки необходимо реализовать функцию, в котором будет определяться компоненты доверенной загрузки.

Таблица 4 - Требования к подсистеме настройки ЗПС

Требования к подсистеме замкнутой программной среды	Низкоуровневые требования
Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения	Реализовать функцию по определению перечня компонентов программного обеспечения запускаемых автоматически при загрузке операционной системы.
	Реализовать функцию, в информационной системе обеспечивается управление временем запуска и завершения работы компонентов программного обеспечения..
Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения	В подсистеме настройки необходимо реализовать настройку параметров установки компонентов программного обеспечения, обеспечивающая исключение установки компонентов программного обеспечения, использование которых не требуется.

Таблица 5 - Требования к подсистеме управления носителями информации

Требования к подсистеме управления носителями информации	Низкоуровневые требования
Контроль использования интерфейсов ввода (вывода) информации	В подсистеме настройки необходимо создать функцию контроля интерфейсов ввода-вывода, регистрация, отключение.
Контроль подключения машинных носителей информации	В подсистеме настройки должна быть реализована функция, осуществляющая контроль машинных носителей разрешенные или запрещенные типы носителей, или же конкретные носители.

Таблица 6 - Требования к подсистеме регистрации и учета

Требования к подсистеме регистрации и учета	Низкоуровневые требования
Определение событий безопасности, подлежащих регистрации, и сроков их хранения	Реализовать функцию по определению типов событий подлежащих регистрации
	Реализовать функцию определения типов данных хранимой информации. А именно о событиях безопасности, всех записей журналов итд. Также определение хранения файлов, журналов, или записей.
Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	В подсистеме настройки необходимо реализовать функцию, определяющую состав и содержание информации о событиях безопасности.

Таблица 7 - Требования к подсистеме контроля целостности

Требования к подсистеме регистрации и учета	Низкоуровневые требования
Контроль целостности информации, содержащейся в базах данных информационной системы	Реализовать функцию установки периодичности контроля целостности базы данных
	Реализовать функцию выбора баз данных для контроля целостности, выбор модулей баз данных.
Ограничение прав пользователей по вводу информации в информационную систему	В подсистеме настройки необходимо реализовать ограничение прав пользователей по вводу информации в ИС. Реализовать выбор объектов файловой системы, объектов баз данных, объектов прикладного и специального программного обеспечения.

7 Проектирование подсистемы настройки средства защиты информации от несанкционированного доступа

7.1 Состав интерфейсов взаимодействия подсистемы настройки с внешними подсистемами

В данном разделе осуществляется разработка подсистемы настройки СЗИ от НСД. Разработка требований осуществляется на основе требований сформулированных в разделе 6.

Как было сказано ранее, требований вытекающих из раздела 6 данного проекта недостаточно для полного функционирования СЗИ от НСД. Существует необходимость в разработке требований, регулирующих сам интерфейс взаимодействия с другими подсистемами.

7.2 Требования к интерфейсу взаимодействия идентификации и аутентификации с подсистемой настройки

Первое высокоуровневое требование это «Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов». К данному требованию можно отнести следующие низкоуровневые требования

- реализовать функцию, где формируется идентификатор пользователя или устройства;
- реализовать функцию исключающую повторное использование идентификатора;
- реализовать функцию, блокирующую идентификатор пользователя через период времени неиспользования;
- реализовать функцию, в которой обеспечивается управление идентификаторами внешних пользователей.

Для формирования пользователя или устройства необходимо создать функцию, сохраняющую идентификационные данные в базу данных. Диаграмма компонентов представлена на рисунке 1.

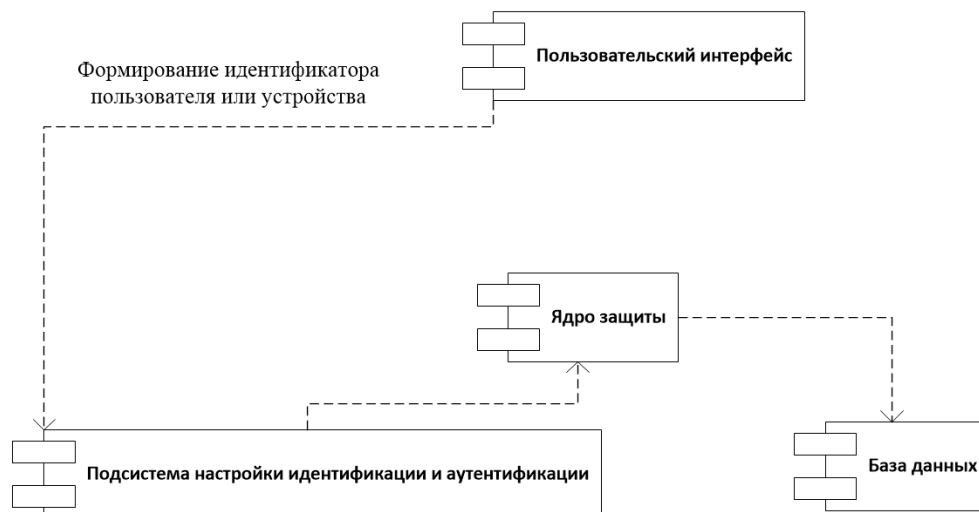


Рисунок 1 - Формирование идентификатора пользователя или устройства

Для исключения повторного использования идентификатора нужно задать необходимые значения (не менее одного года; не менее трех лет; в течение всего периода эксплуатации информационной системы;) и реализовать функцию сохраняющую настройки в базу данных. Диаграмма компонентов представлена на рисунке 2.

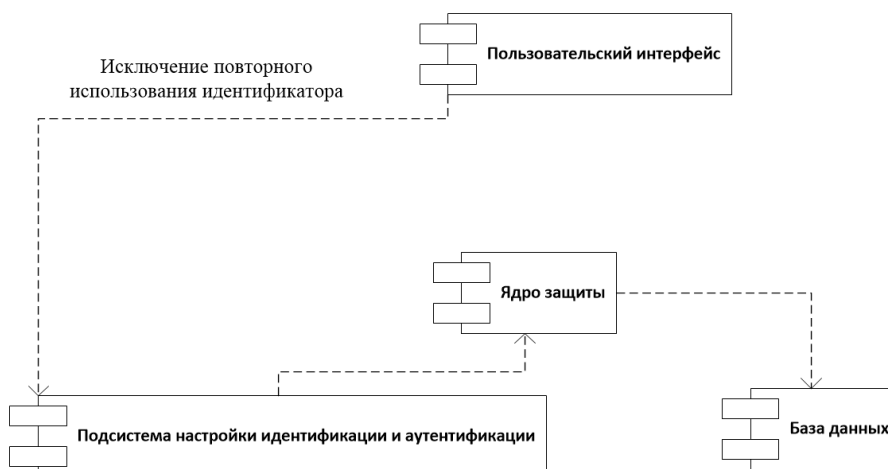


Рисунок 2 - Исключение повторного использования идентификатора

Для блокировки идентификатора пользователя необходимо задать значение (не более 90 дней, не более 45 дней) и реализовать функцию сохраняющую данные настройки в базу данных. Диаграмма компонентов представлена на рисунке .3.

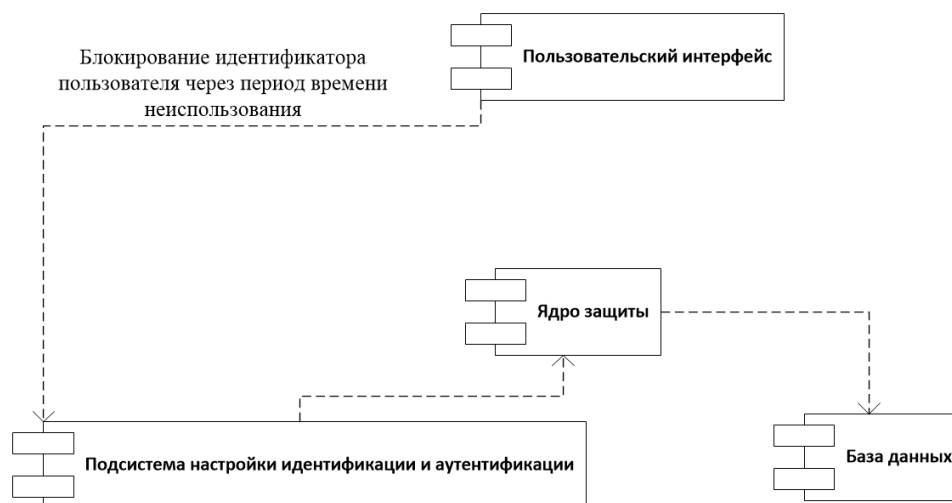


Рисунок 3 - Блокирование идентификатора пользователя через период времени неиспользования

Следующее высокоуровневое требование «Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации». К данному требованию можно отнести следующие низкоуровневые требования:

- изменение аутентификационной информации;
- изменение характеристик пароля;
- установка времени блокировки в случае неуспешного ввода;
- промежуток времени на смену пароля.

Для изменения аутентификационной информации, необходимо создать функцию, сохраняющую изменения в базу данных. Диаграмма компонентов представлена на рисунке 4.

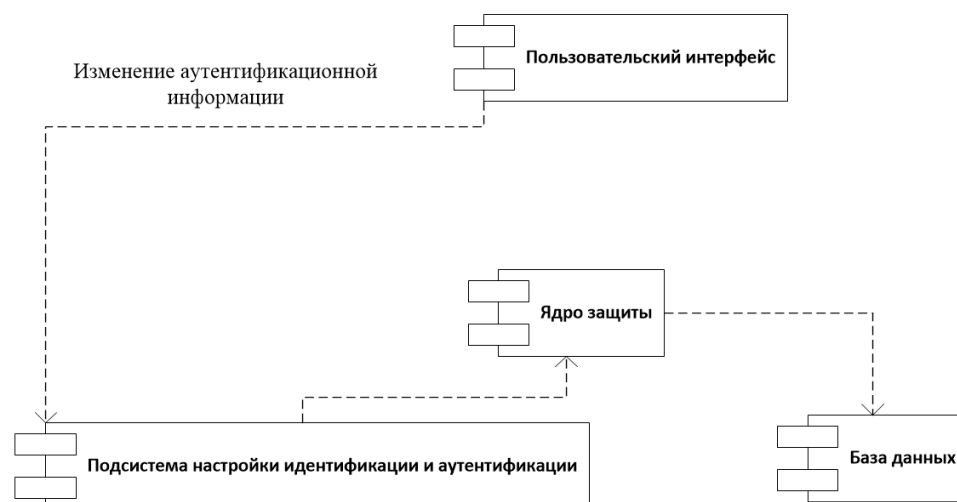


Рисунок 4 - Изменение аутентификационной информации

Для изменения характеристик пароля необходимо задать значения длины пароля (не менее 6 символов), алфавит пароля (не менее 30 символов), количество неуспешных попыток и необходимо реализовать функцию сохранения настроек в базу данных. Диаграмма компонентов представлена на рисунке 5.

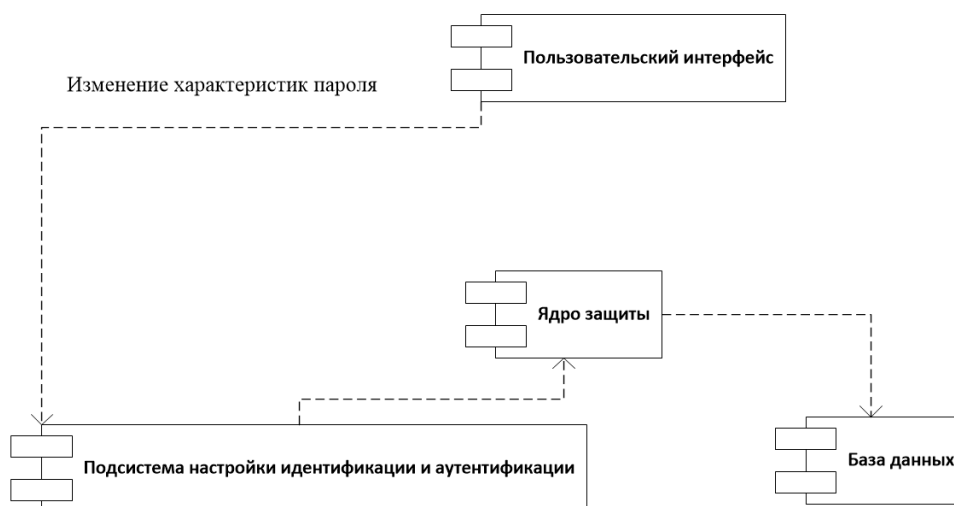


Рисунок 5 - Диаграмма компонентов «Изменение характеристик пароля»

Для установки времени блокировки в случае неуспешного ввода (от 3 до 60) необходимо реализовать функцию сохранения настроек в базу данных. Диаграмма компонентов представлена на рисунке 6.

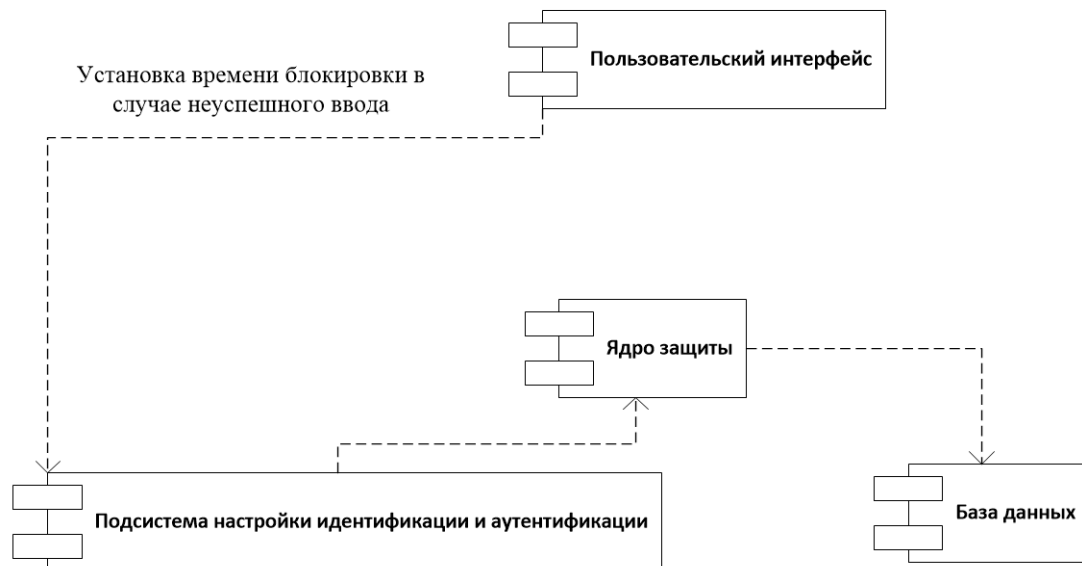


Рисунок 6 - Установка времени блокировки в случае неуспешного ввода

Для промежутка времени на смену пароля необходимо реализовать функцию выбора времени и сохранения данных настроек. Диаграмма компонентов представлена на рисунке 7.

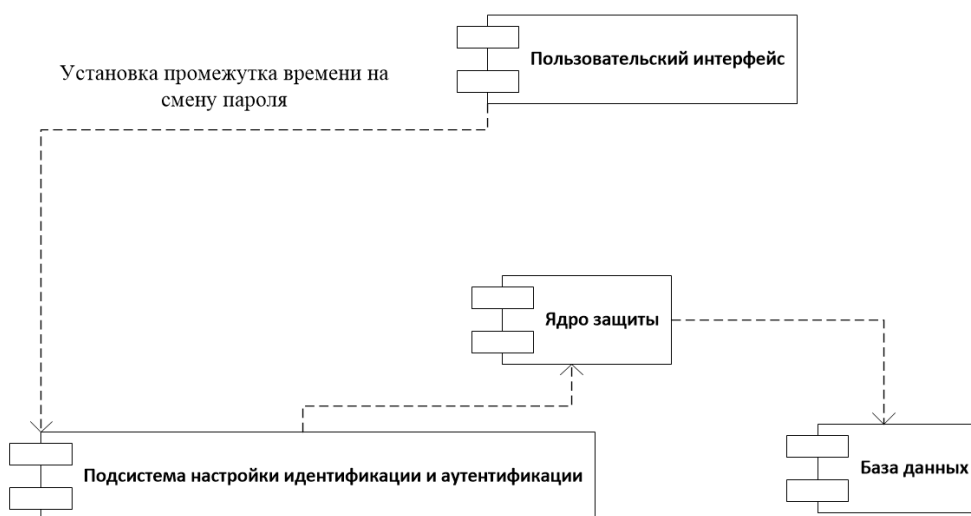


Рисунок - Установка промежутка времени на смену пароля

7.3 Требования к интерфейсу взаимодействия подсистемы управления доступом с подсистемой настройки

Первое высокоуровневое требование это «Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей». К данному требованию можно отнести следующие низкоуровневые требования:

- определение типа учетной записи;
- группирование учетных записей;
- заведение, активации , блокирования и уничтожения учетных записей пользователей;
- корректировки учетных записей;
- определение срока актуальности временной учетной записи;
- автоматическое блокирование неиспользуемых учетных записей;
- блокирования учетных записей.

Для определения типа учетной записи необходимо выбрать тип учетной записи (внутренний пользователь, внешний пользователь, гость, временная учетная запись и предоставить возможность создавать свои типы пользователей) и сохранить настройку в базу данных СЗИ от НСД. Диаграмма компонентов представлена на рисунке 8.

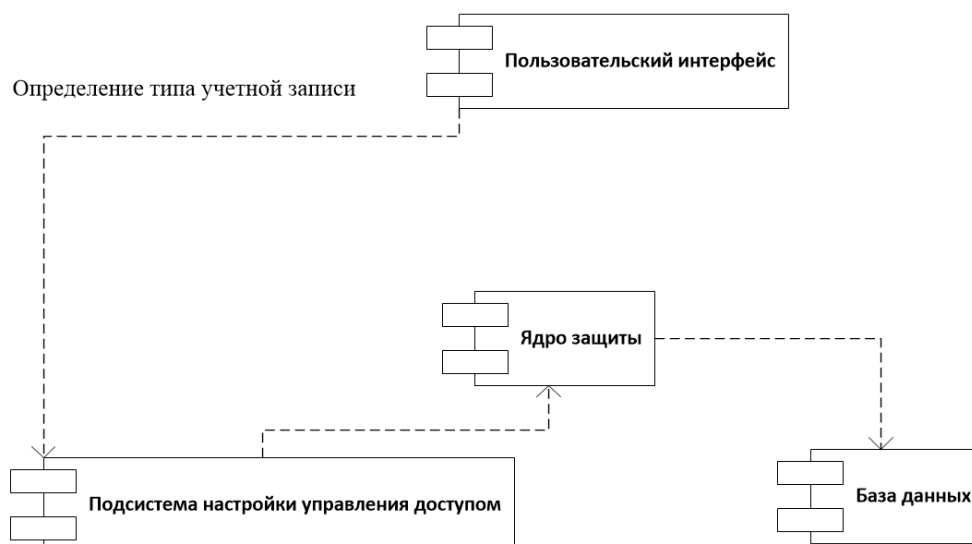


Рисунок 8 - Определение типа учетной записи

Для группирования учетных записей, необходимо нужной учетной записи определить группу к которой она принадлежит, и сохранить настройки в базу данных СЗИ от НСД. Диаграмма компонентов представлена на рисунке 9.

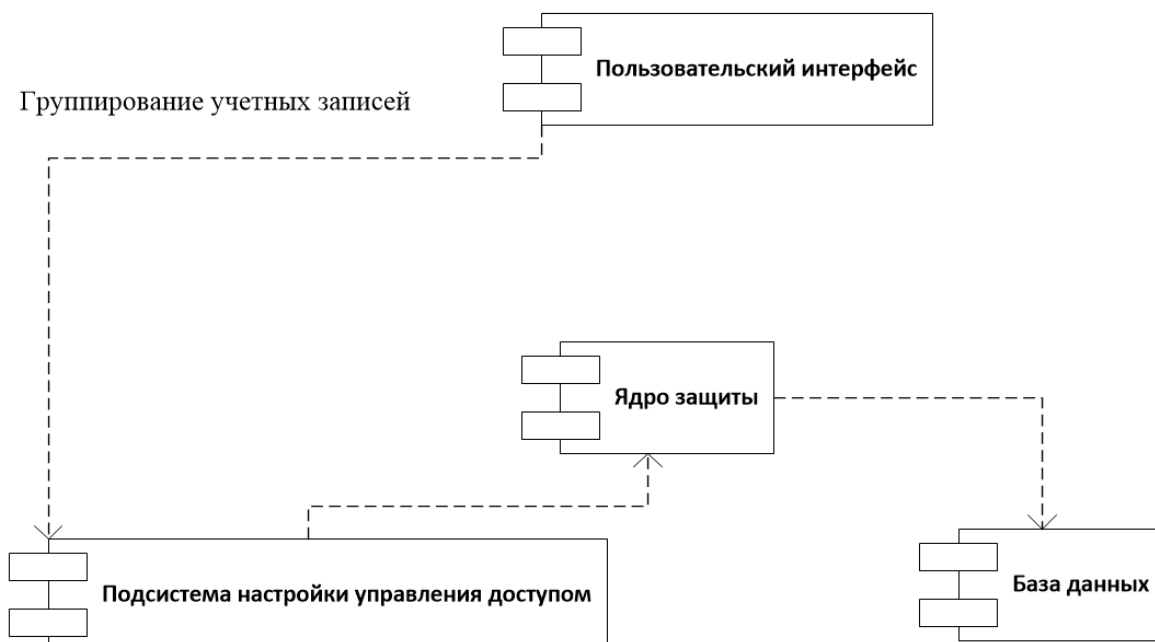


Рисунок 9 - Группирование учетных записей

Для заведения, активации, блокирования и уничтожения учетных записей пользователей необходимо задать соответствующие функции, а также реализовать функцию сохранения данных настроек. Диаграмма компонентов представлена на рисунке 10.

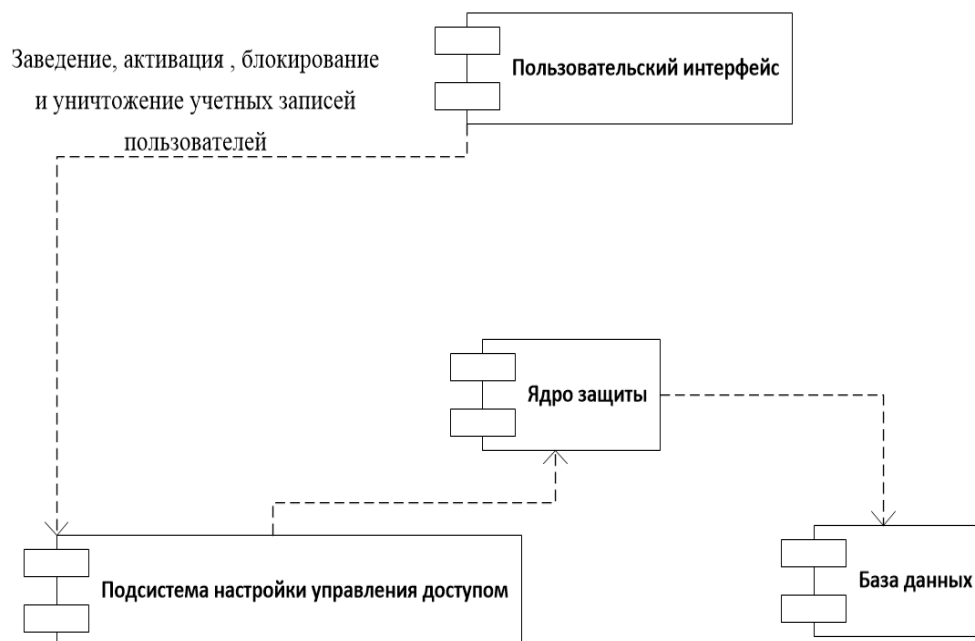


Рисунок 10 - Заведение, активация , блокирование и уничтожение учетных записей пользователей

Для корректировки учетных записей необходимо реализовать функцию изменения учетных записей и сохранения результатов в базу данных. Диаграмма компонентов представлена на рисунке 11.

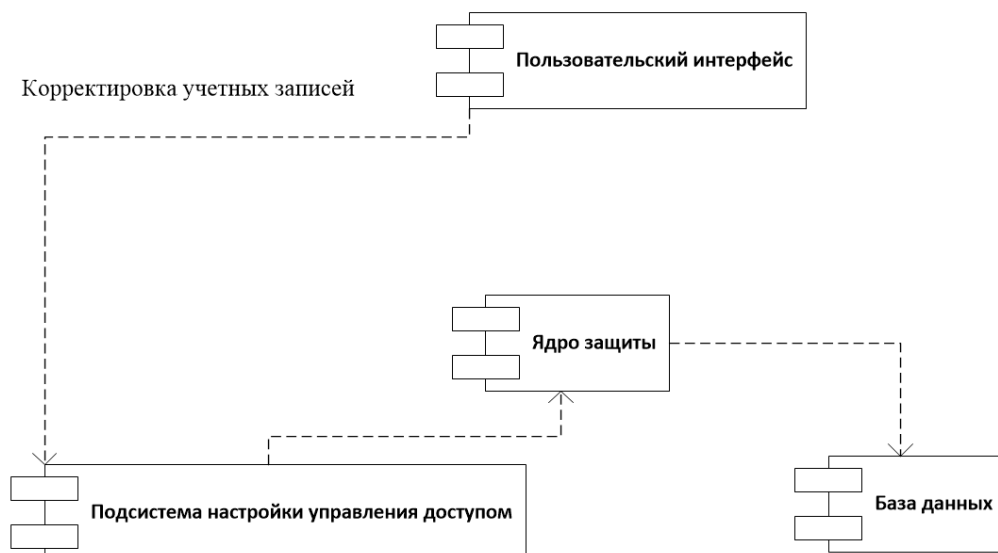


Рисунок 11 - Корректировка учетных записей

Для определения срока актуальности временной учетной записи необходимо задать нужное значение, и сохранить настройки данной учетной записи в базу данных. Диаграмма компонентов представлена на рисунке 12



Рисунок 12 - Определение срока актуальности временной учетной записи

Для автоматического блокирования неиспользуемых учетных записей, необходимо задать временные значения (более 90 дней, более 45 дней) и реализовать функцию сохранения данной настройки. Диаграмма компонентов представлена на рисунке 13.



Рисунок 13 - Автоматическое блокирование неиспользуемых учетных записей

Для автоматической блокировки учетных записей необходимо задать количество неуспешных попыток аутентификации, а также задать события безопасности которые будут причиной блокировки. Данные события безопасности могут быть заимствованы из настроек журнала событий. Также необходимо реализовать функцию сохранения данной настройки. Диаграмма компонентов представлена на рисунке 14



Рисунок 14 - Блокирование учетных записей

Следующее высокоуровневое требование это «Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа». К данному требованию можно отнести следующие низкоуровневые требования:

- дискреционный метод разграничения;
- мандатного метод разграничения.

Для дискреционного метода разграничения доступа необходимо задать количество субъектов и объектов ИБ. Для простоты использования необходимо реализовать функцию заимствования групп учетных записей пользователей и использовать данные группы в качестве субъекта ИБ, а также для определения объектов ИБ, в целях экономии времени необходимо использовать шаблон защищаемых системных файлов, а также шаблон используемых субъектом файлов, экспортированных из подсистемы регистрации и учета. Также необходимо реализовать функцию сохранения настроек в БД. Диаграмма компонентов представлена на рисунке 15.

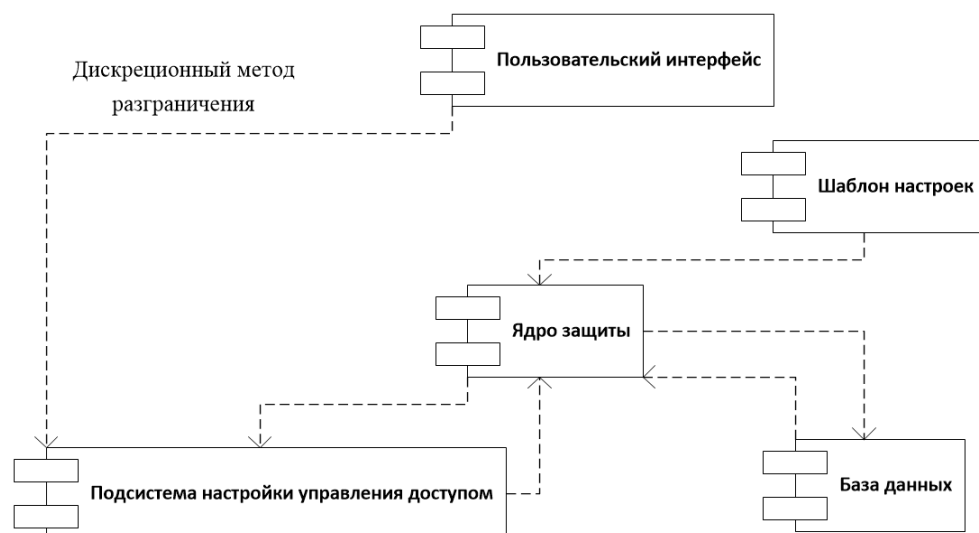


Рисунок 15 - Дискреционный метод разграничения

Для мандатного разграничения доступа необходимо задать для защищаемых ресурсов - гриф секретности, для пользователей – уровень допуска. Для удобства необходимо добавить возможность заимствовать группы учетных записей. А также метки безопасности назначенные администратором. Также необходимо реализовать функцию, сохранения настроек в базу данных. Диаграмма компонентов представлена на рисунке 16.

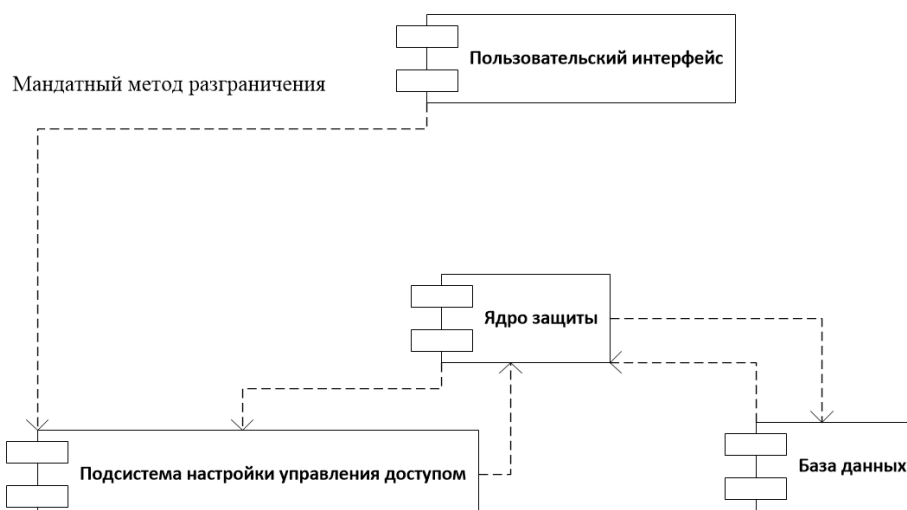


Рисунок 16 - Мандатный метод разграничения

Следующее высокоуровневое требование это «Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы». К данному требованию можно отнести низкоуровневое требование «Разграничение ролей (администрирование, мониторинг, обработка информации) » необходимо выбрать роль пользователя, также есть возможность интеграции групп пользователей. Необходимо реализовать функцию по сохранению данных настроек. Диаграмма компонентов представлена на рисунке 17

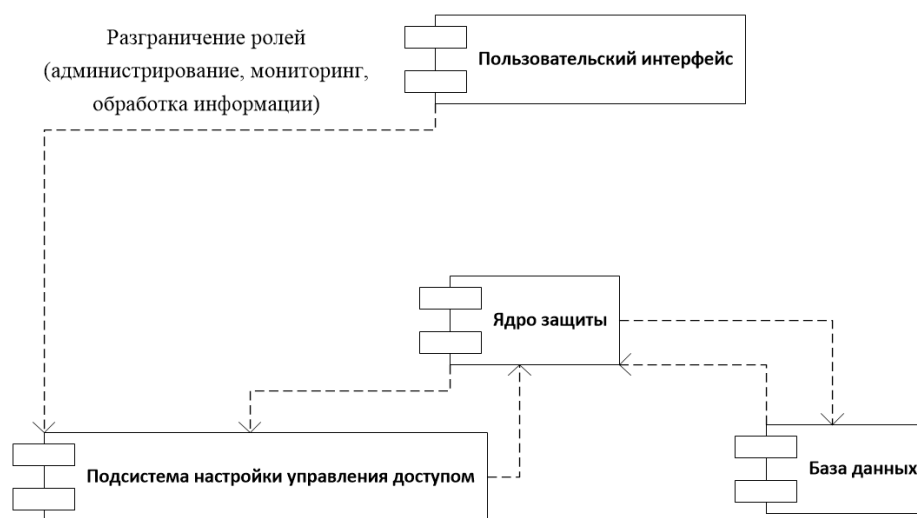


Рисунок 17 - Разграничение ролей (администрирование, мониторинг, обработка информации)

Следующее высокоуровневое требование «Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы». Из данного требования вытекает низкоуровневое требование «Предоставление прав к функциям безопасности» необходимо выбрать тип пользователя (администратор, оператор итд) или группу пользователей. Определить права данных меток, и их запреты. Привилегии могут вводиться как в ручную, так и при интеграции шаблона настроек к данным группам пользователей.

Необходимо создать функцию сохранения настроек в базах данных. Диаграмма компонентов представлена на рисунке 18

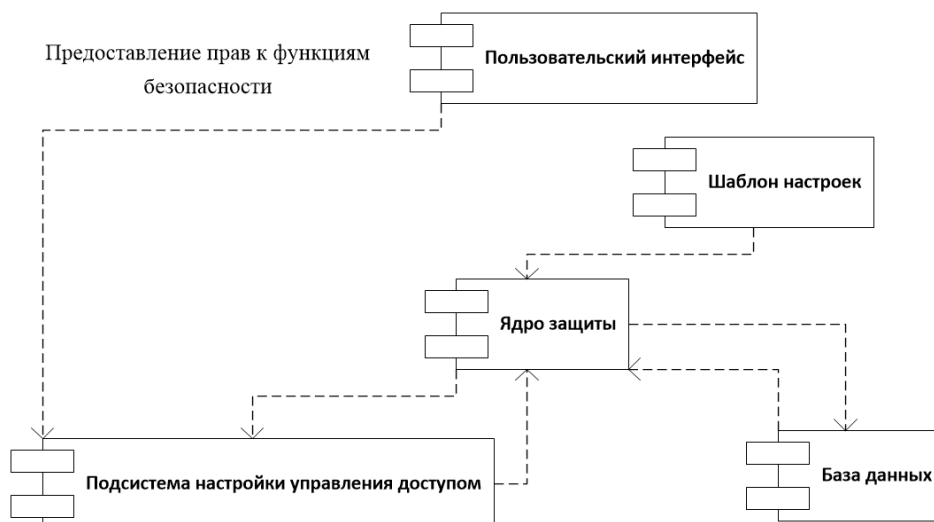


Рисунок 18 - Предоставление прав к функциям безопасности

Следующее высокоуровневое требование «Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)» к данному высокоуровневому требованию относятся :

- ограничение неуспешных попыток входа в информационную систему;
- разблокировка учетной записи .

Для ограничения неуспешных попыток входа в ИС, необходимо задать функцию задания максимального количества попыток входа. Также необходимо создать функцию по сохранению настроек в базу данных. Диаграмма компонентов представлена на рисунке 19.

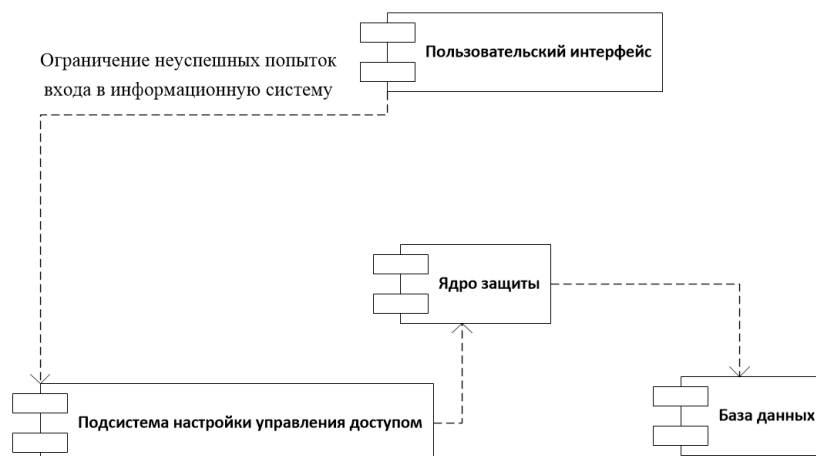


Рисунок 19 - Ограничение неуспешных попыток входа в информационную систему

Для разблокировки учетной записи необходимо реализовать функцию разблокировки учетной записи, а также сохранения настроек в базу данных. Диаграмма компонентов представлена на рисунке 20.

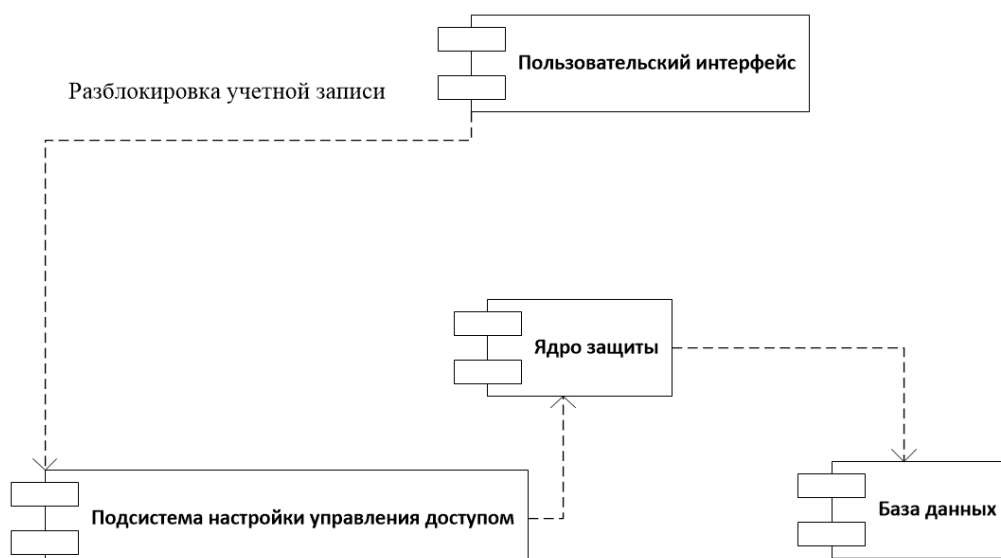


Рисунок 20 - Разблокировка учетной записи

Высокоуровневое требование «Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу» из данного требования

вытекает низкоуровневое требование «Определение времени бездействия пользователя». В данной функции необходимо задать значения (до 15 минут, до 5 минут) по истечении времени происходит завершение сеанса пользователя. Также необходимо задать функцию сохранения настроек. Диаграмма компонентов представлена на рисунке 21.

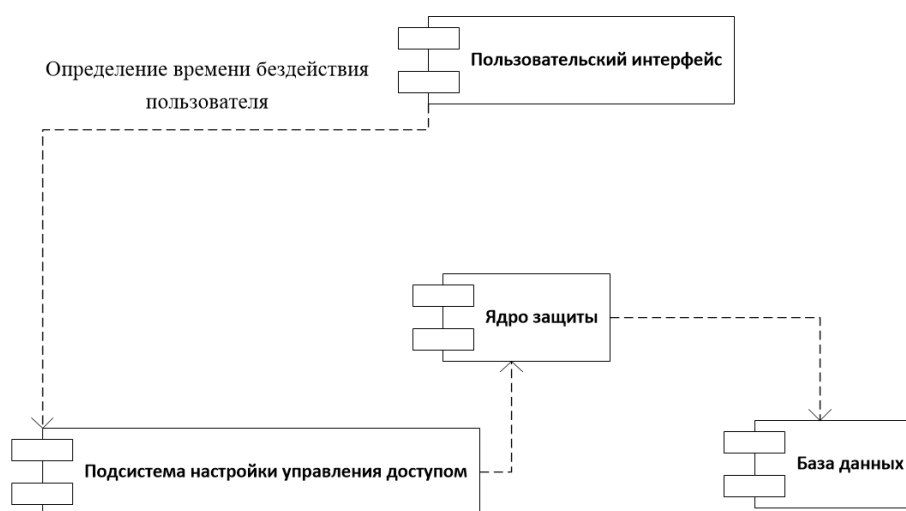


Рисунок 21 - Определение времени бездействия пользователя

Следующее высокоуровневое требование «Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации». Из данного требования вытекает низкоуровневое требование «Выбор количества действий разрешенных до идентификации и аутентификации.» В данной функции необходимо задать действия разрешенные до входа. А также реализовать функцию сохранения настроек . Диаграмма компонентов представлена на рисунке 22.

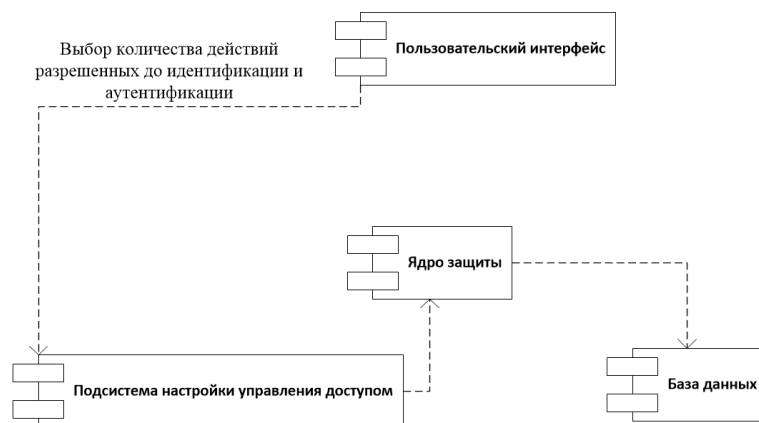


Рисунок 22 - Выбор количества действий разрешенных до идентификации и аутентификации

Высокоуровневое требование «Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки». Из данного требования вытекает низкоуровневое требование «Обновление, назначение, изменение и сохранение атрибутов безопасности (меток безопасности)». Необходимо реализовать функцию, сохраняющую настройки в базу данных. Диаграмма компонентов представлена на рисунке 23.

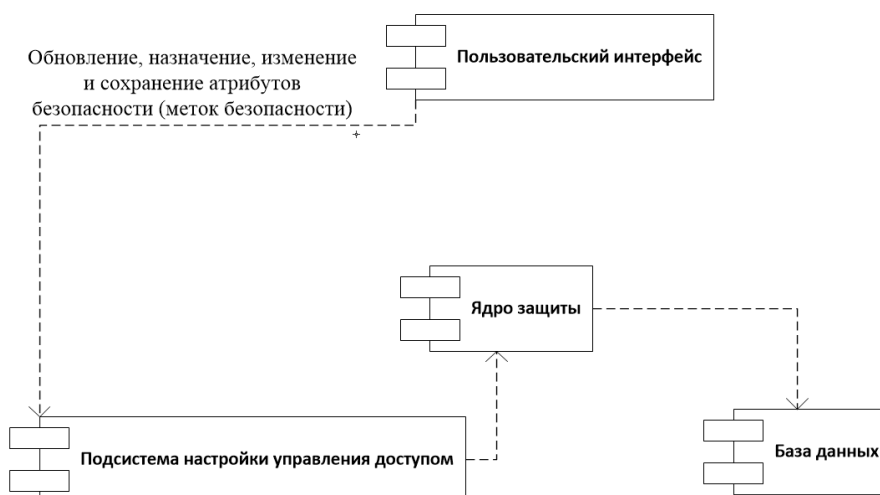


Рисунок - 23 Обновление, назначение, изменение и сохранение атрибутов безопасности (меток безопасности)

Высокоуровневое требование «Регламентация и контроль использования в информационной системе мобильных технических средств». Из данного требования вытекает низкоуровневое требования:

- регламентация мобильных технических средств;
- контроль мобильных технических средств.

Для регламентации мобильных технических средств, необходимо создать список разрешенных средств с присвоенными к ним идентификаторами. Необходимо создать функцию сохраняющую данные настройки. Диаграмма компонентов представлена на рисунке 24.

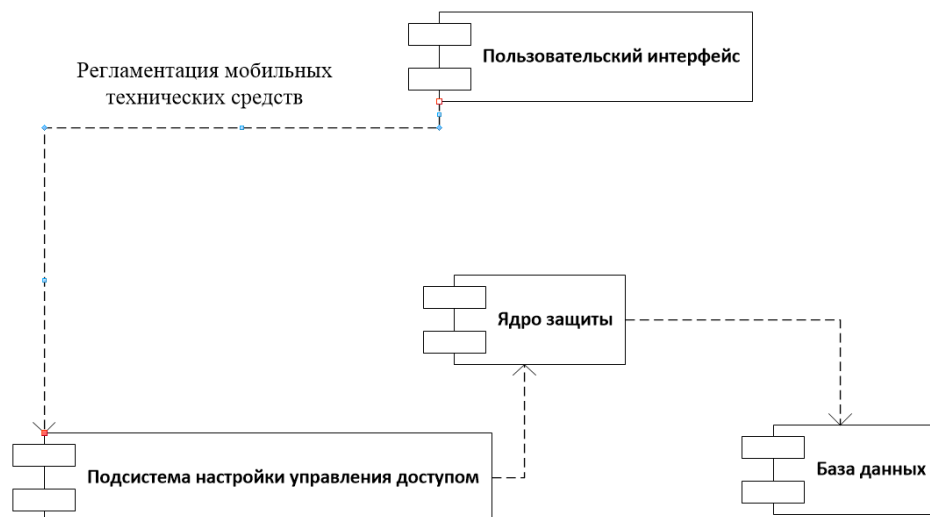


Рисунок 24 - Регламентация мобильных технических средств

Для контроля мобильных технических средств. Необходимо внедрить функцию регистрации технических средств. А также функция запрета или разрешения доступа к данному техническому средству. Также создать функцию сохранения настроек. Диаграмма компонентов представлена на рисунке 25

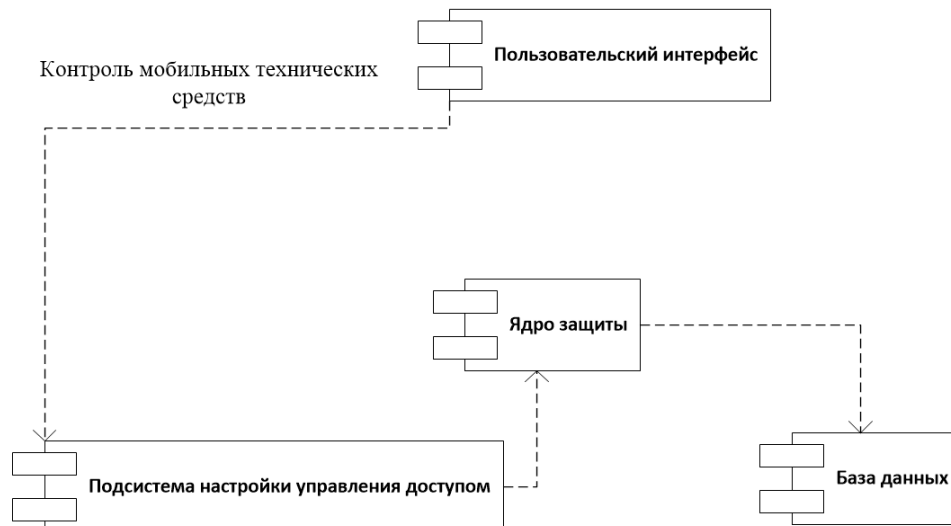


Рисунок 25 - Контроль мобильных технических средств

Высокоуровневое требование «Обеспечение доверенной загрузки средств вычислительной техники». Из данного требования вытекает низкоуровневое требование «Определение компонентов доверенной загрузки» которые определяются в ручную или же интегрируются файлом от разработчика. Необходимо реализовать функцию по сохранению данных настроек. Диаграмма компонентов представлена на рисунке 26

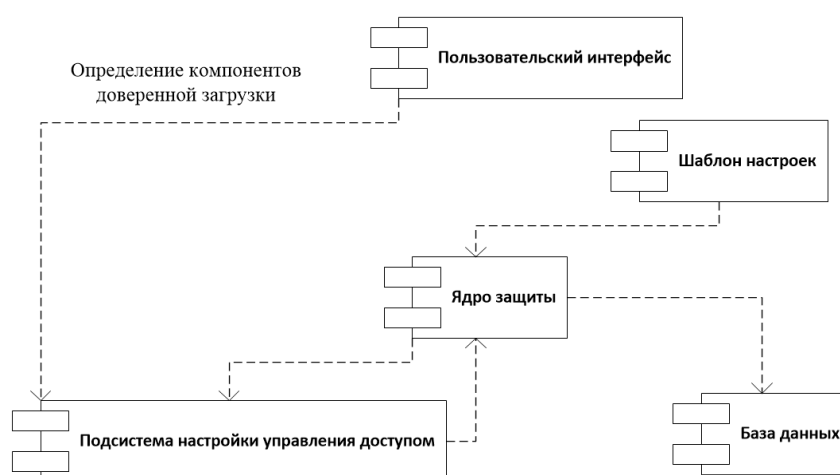


Рисунок 26 - Определение компонентов доверенной загрузки

7.4 Требования к интерфейсу взаимодействия подсистемы замкнутой программной среды с подсистемой настройки

Высокоуровневое требование «Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения» из которого вытекают следующие низкоуровневые требования:

- определение перечня компонентов программного обеспечения (файлов, объектов баз данных, хранимых процедур и иных компонентов), запускаемых автоматически при загрузке операционной системы;
- управление временем запуска и завершения работы компонентов программного обеспечения.

Для определения перечня необходимо создать функцию выбора перечня, а также сохранения результатов настроек. Диаграмма компонентов представлена на рисунке 27.

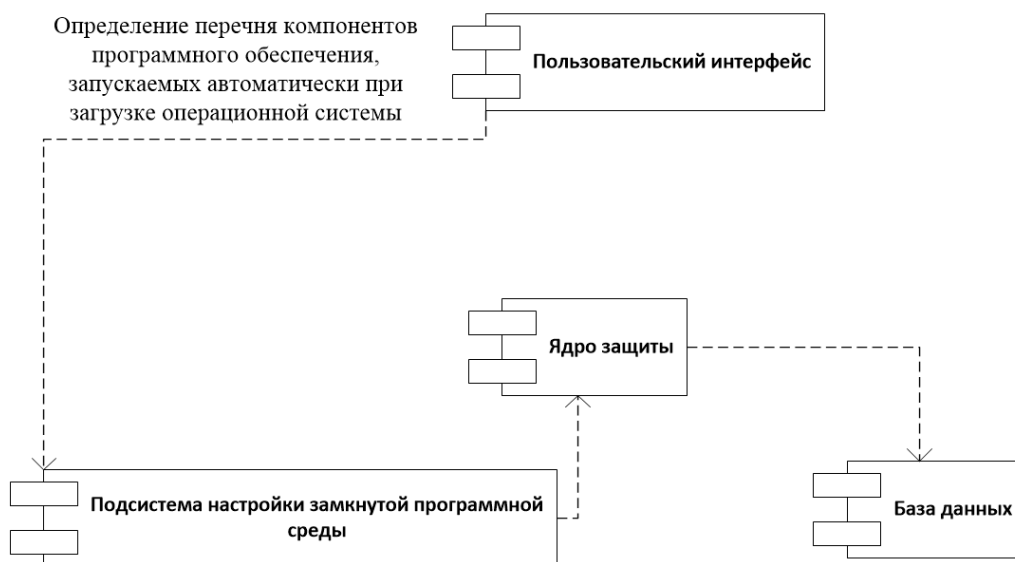


Рисунок 27 - Определение перечня компонентов программного обеспечения, запускаемых автоматически при загрузке операционной системы

Для управления временем запуском, необходимо выбрать время запуска и сохранить настройку. Диаграмма компонентов представлена на рисунке 28



Рисунок 28 - Управление временем запуска и завершения работы компонентов программного обеспечения

Высокоуровневое требование «Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения». Из которого вытекает низкоуровневое требование «Настройку параметров установки компонентов программного обеспечения, обеспечивающая исключение установки (если осуществимо) компонентов программного обеспечения, использование которых не требуется». В данной функции необходимо реализовать выбор компонентов и сохранение параметров в базу данных. Диаграмма компонентов представлена на рисунке 29.



Рисунок 29 - Настройка параметров установки компонентов программного обеспечения

7.5 Требования к интерфейсу взаимодействия управления носителями информации с подсистемой настройки

Первое высокоуровневое требование «Контроль использования интерфейсов ввода (вывода) информации». Из которого вытекает низкоуровневое требование «Ограничение использования интерфейсов ввода – вывода» Необходимо реализовать функцию отключения запрещенных интерфейсов. Их регистрация и сохранения данных настроек. Диаграмма компонентов представлена на рисунке 30.

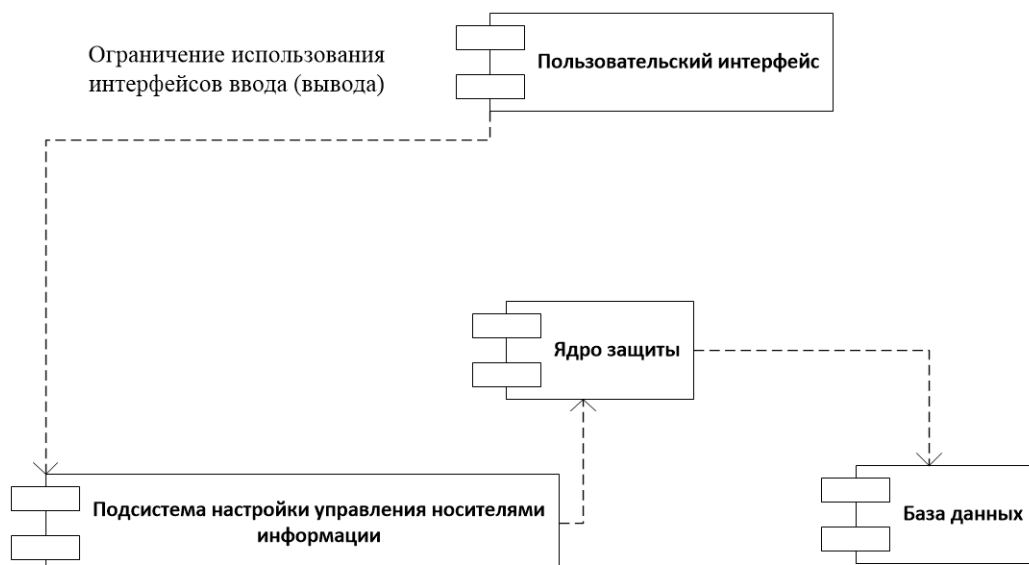


Рисунок 30 - Ограничение использования интерфейсов ввода (вывода)

Далее высокоуровневое требование «Контроль подключения машинных носителей информации» из которого вытекает низкоуровневое требование «контроль машинных носителей (разрешенные или запрещенные типы носителей, или же конкретные носители.)». Необходимо реализовать данную функцию по определению типов носителей и сохранению настроек в базу данных. Диаграмма компонентов представлена на рисунке 31.

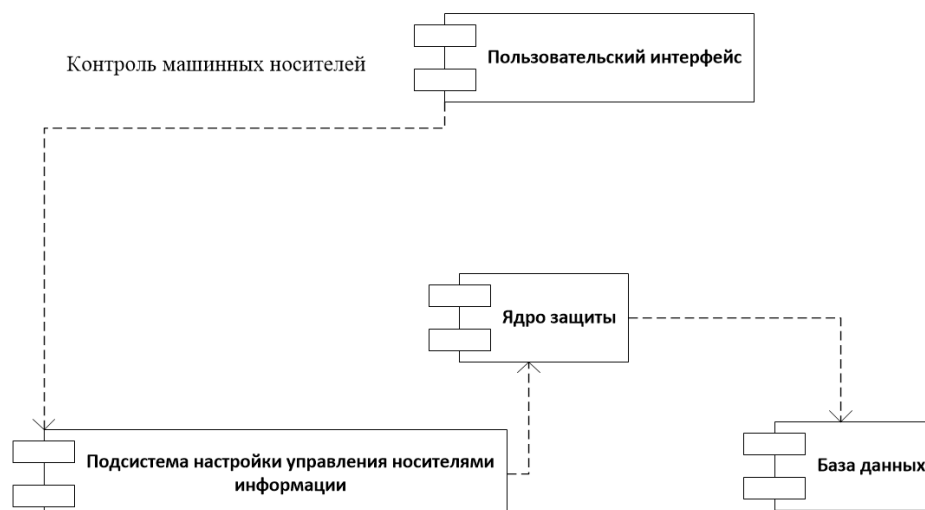


Рисунок 31. Контроль машинных носителей

7.6 Требования к интерфейсу взаимодействия регистрации и учета с подсистемой настройки

Первое высокоуровневое требование «Определение событий безопасности, подлежащих регистрации, и сроков их хранения» к которому можно отнести следующие низкоуровневые требования:

- Определение типов событий подлежащих регистрации
- Определения типов данных хранимой информации

Для определения типов событий подлежащих регистрации, необходимо задать функцию по выбору данных событий, а также сохранению данных настроек. Диаграмма компонентов представлена на рисунке 32

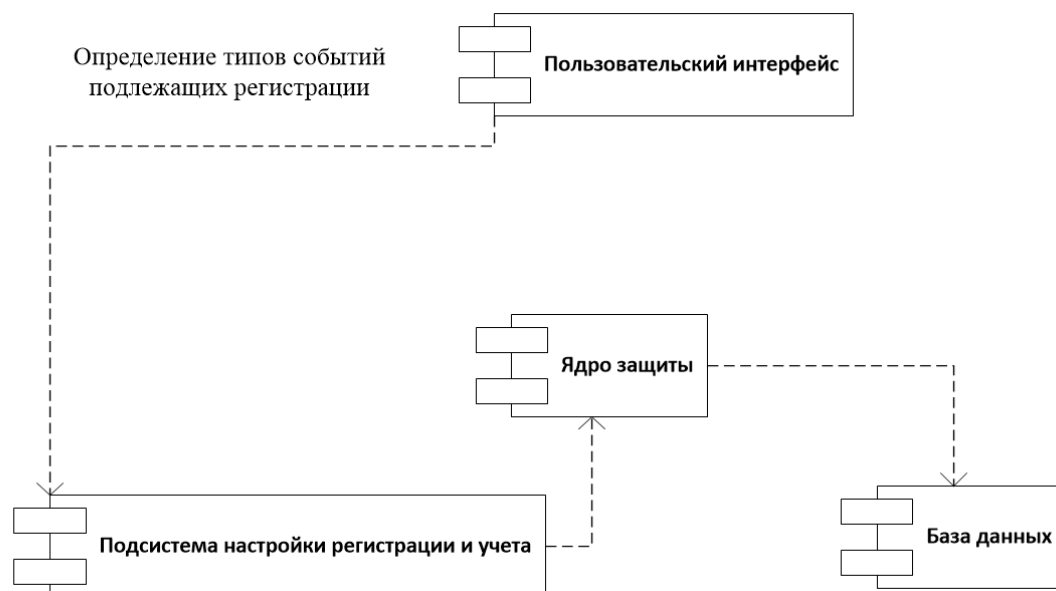


Рисунок 32 - Определение типов событий подлежащих регистрации

Для определения типов данных необходимо реализовать функцию выбора места сохранения журналов, и типов сохраняемой информации. Настройки данных журналов необходимо сохранить в базу данных. Диаграмма компонентов представлена на рисунке 33.

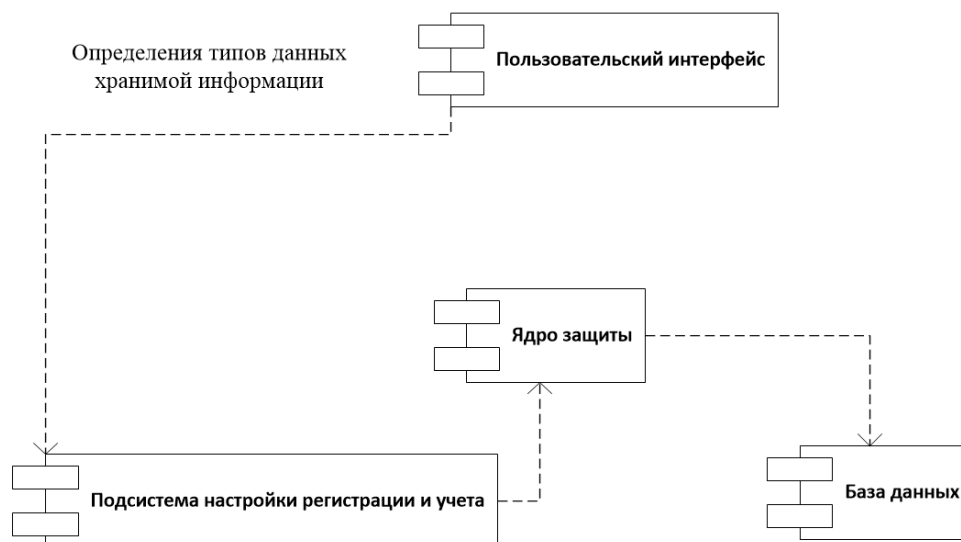


Рисунок 33 - Определения типов данных хранимой информации

Следующее высокоуровневое требование «Определение состава и содержания информации о событиях безопасности, подлежащих регистрации», из которого вытекает требование «Определение состава и содержания информации о событиях безопасности». Данное требование реализуется путем выбора информации из списка предлагаемым разработчиком, а также функцией сохранения настроек. Диаграмма компонентов представлена на рисунке 34

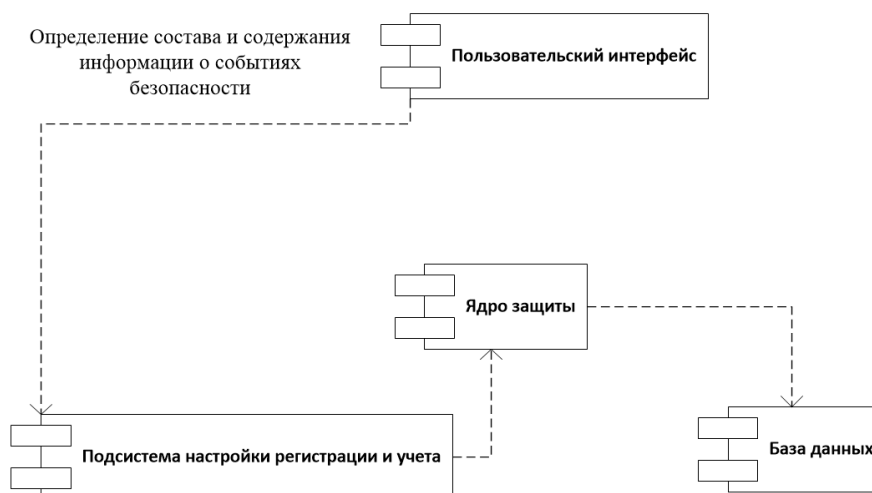


Рисунок 34 - Определение состава и содержания информации о событиях безопасности

7.7 Требования к интерфейсу взаимодействия контроля целостности с подсистемой настройки

Высокоуровневое требование «Контроль целостности информации, содержащейся в базах данных информационной системы». Из данного требования вытекает низкоуровневое требования :

- установка периодичности контроля целостности базы данных;
- выбор баз данных для контроля целостности, выбор модулей баз данных.

Установка периодичности контроля целостности базы данных реализуется выбором периодичности и функцией сохранения настроек. Диаграмма компонентов представлена на рисунке 35.

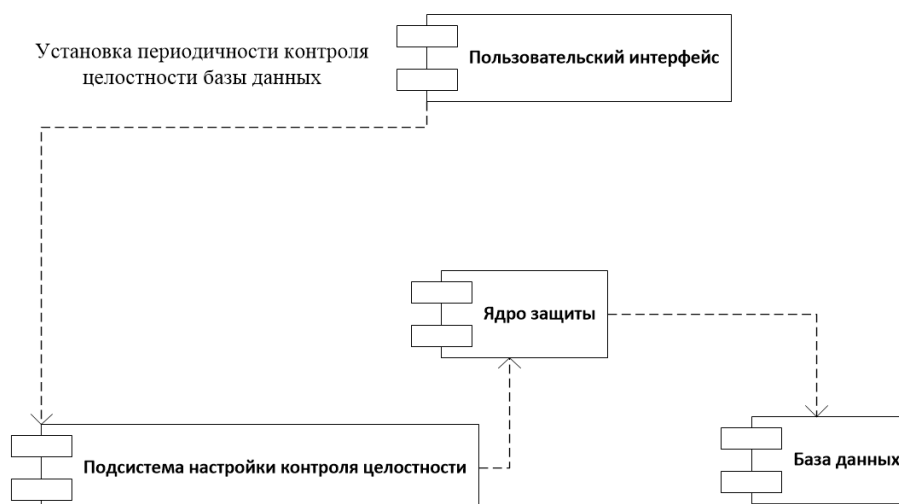


Рисунок 35 - Установка периодичности контроля целостности базы данных

Выбор баз данных для контроля целостности, выбор модулей баз данных. Реализуется выбором базы данных и функцией по сохранению данных настроек. Диаграмма компонентов представлена на рисунке 36.

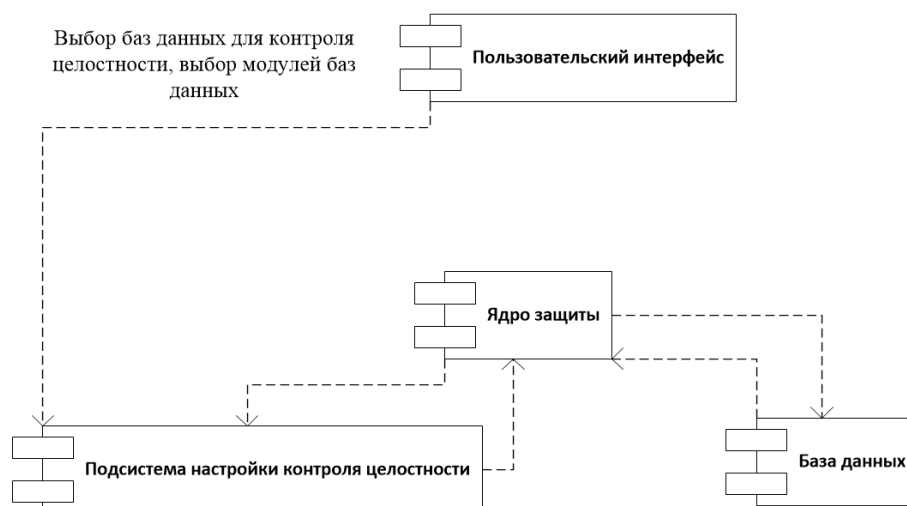


Рисунок 36 - Выбор баз данных для контроля целостности, выбор модулей баз данных

Высокоуровневое требование «Ограничение прав пользователей по вводу информации в информационную систему», из которого вытекает низкоуровневое требование «Выбор объектов файловой системы, объектов баз данных, объектов прикладного и специального программного обеспечения.» Список баз данных и объектов можно импортировать с других подсистем. Также необходимо реализовать функцию по сохранению данных настроек. Диаграмма компонентов представлена на рисунке 37.

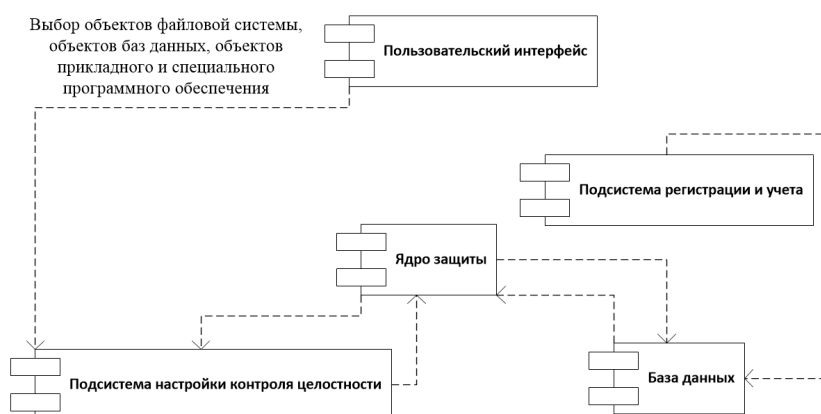


Рисунок 37 - Выбор объектов файловой системы, объектов баз данных, объектов прикладного и специального программного обеспечения

Разноуровневые требования к подсистеме настройки приведены в таблице

8.

Таблица 8 – Дополнительные требования к подсистеме настройки СЗИ от НСД

Высокоуровневое требование	Низкоуровневое требование	Дополнительное требование
Подсистема настройки идентификации и аутентификации		
Управление идентификаторами	Формирование идентификатор пользователя или устройства.	Сохранение результатов настройки
	Исключение повторного использования идентификатора	Выбор временного значения
		Сохранение результатов настройки
	Блокирование идентификатора пользователя через период времени неиспользования	Выбор временного значения
		Сохранение результатов настройки
Управление средствами аутентификации	Изменение аутентификационной информации	Сохранение результатов настройки
	Изменение характеристик пароля	Выбор длины пароля
		Выбор алфавита пароля
		Выбор количества неуспешных попыток ввода
		Сохранение результатов настройки
	Установка времени блокировки в случае неуспешного ввода	Выбор времени блокировки
		Сохранение результатов настройки
	Установка промежутка времени на смену пароля	Выбор промежутка времени на смену

Продолжение таблицы 8 – Дополнительные требования к подсистеме настройки СЗИ от НСД

Высокоуровневое требование	Низкоуровневое требование	Дополнительное требование
		пароля
		Сохранение результатов настройки
Подсистема настройки управления доступом		
Управление учетными записями пользователей, в том числе внешних пользователей	Определение типа учетной записи	Выбор типа учетной записи
		Сохранение результатов настройки
	Группирование учетных записей	Создание/удаление групп пользователей
		Сохранение результатов настройки
	Заведение, активация , блокирование и уничтожение учетных записей пользователей.	Выбор действий с учетными записями
		Сохранение результатов настройки
	Корректировка учетных записей	Сохранение результатов настройки
	Определение срока актуальности временной учетной записи	Выбор срока актуальности
		Сохранение результатов настройки
	Автоматическое блокирование неиспользуемых учетных записей	Выбор срока блокирования
		Сохранение результатов настройки
	Блокирования учетных записей	Выбор количества неуспешных попыток аутентификации
		Выбор событий безопасности
		Интеграция событий безопасности из

Продолжение таблицы 8 – Дополнительные требования к подсистеме настройки СЗИ от НСД

Высокоуровневое требование	Низкоуровневое требование	Дополнительное требование
Реализация необходимых методов), типов и правил разграничения доступа	Дискреционный метод разграничения	настроек журнала регистрации
		Сохранение результатов настройки
		Выбор субъектов и объектов ИБ
		Выбор групп пользователей
		Импорт настроек из шаблона защищаемых файлов
	Мандатный метод разграничения	Импорт используемых объектов из подсистемы регистрации и учета
		Сохранение результатов настройки
		Выбор грифа секретности и уровня допуска
		Интеграция меток безопасности
		Интеграция групп пользователей
		Сохранение результатов настройки
	Разграничение ролей	Выбор ролей
		Интеграция групп пользователей
		Сохранение результатов настройки
Назначение минимально необходимых	Предоставление прав к функциям безопасности	Выбор типа пользователя и привелегий

Продолжение таблицы 8 – Дополнительные требования к подсистеме настройки СЗИ от НСД

Высокоуровневое требование	Низкоуровневое требование	Дополнительное требование
прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы		Интеграция групп пользователей
		Интеграция шаблона настроек
		Сохранение результатов настроек
Ограничение неуспешных попыток входа в информационную систему.	Ограничение неуспешных попыток входа в информационную систему	Выбор количества неуспешных попыток ввода
		Сохранение результатов настройки
	Разблокировка учетной записи	Сохранение результатов настройки
Блокирование сеанса доступа в информационную систему после установленного времени бездействия пользователя	Определение времени бездействия пользователя	Выбор времени блокировки
		Сохранение результатов настройки
Разрешение действий пользователей, разрешенных до идентификации и аутентификации	Выбор количества действий разрешенных до идентификации и аутентификации	Сохранение результатов настройки
Поддержка и сохранение атрибутов безопасности, связанных с информацией в процессе ее хранения и обработки	Обновление, назначение, изменение и сохранение атрибутов безопасности	Сохранение результатов настройки

Продолжение таблицы 8 – Дополнительные требования к подсистеме настройки СЗИ от НСД

Высокоуровневое требование	Низкоуровневое требование	Дополнительное требование
Регламентация и контроль использования в информационной системе мобильных технических средств	Регламентация мобильных технических средств	Выбор технических средств
		Сохранение результатов настройки
	Контроль мобильных технических средств	Функция запрета к данному техническому средству
		Сохранение результатов настройки
Обеспечение доверенной загрузки средств вычислительной техники	Определение компонентов доверенной загрузки	Выбор компонентов доверенной загрузки
		Импорт настроек с шаблона разработчика
		Сохранение результатов настроек
Подсистема настройки замкнутой программной среды		
Управление запуском компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения	Определение перечня компонентов программного обеспечения запускаемых автоматически при загрузке операционной системы	Выбор перечня компонентов ПО
		Сохранение результатов настройки
	Управление временем запуска и завершения работы компонентов программного обеспечения	Выбор времени запуска
		Сохранение результатов настроек
Управление установкой компонентов	Настройка параметров установки компонентов	Выбор компонентов

Продолжение таблицы 8 – Дополнительные требования к подсистеме настройки СЗИ от НСД

Высокоуровневое требование	Низкоуровневое требование	Дополнительное требование
программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения	программного обеспечения, обеспечивающая исключение установки компонентов программного обеспечения, использование которых не требуется	Сохранение результатов настроек
Подсистема настройки управления носителями информации		
Контроль использования интерфейсов ввода (вывода) информации	Ограничение использования интерфейсов ввода (вывода)	Выбор интерфейсов
		Сохранение результатов настройки
Контроль подключения машинных носителей информации	Контроль машинных носителей	Выбор машинных носителей и действий запрет/разрешение
		Сохранение результатов настройки
Подсистема настройки регистрации и учета		
Определение событий безопасности, подлежащих регистрации, и сроков их хранения	Определение типов событий подлежащих регистрации	Выбор типов данных
		Сохранение результатов настроек
	Определения типов данных хранимой информации	Выбор типов данных и сохранение настроек типов
		Выбор места сохранения журналов

Продолжение таблицы 8 – Дополнительные требования к подсистеме настройки СЗИ от НСД

Высокоуровневое требование	Низкоуровневое требование	Дополнительное требование
Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	Определение состава и содержания информации о событиях безопасности	Выбор из списка событий безопасности
		Сохранение результатов настройки
Подсистема настройки контроля целостности		
Контроль целостности информации, содержащейся в базах данных информационной системы	Установка периодичности контроля целостности базы данных	Выбор периодичности
		Сохранение результатов настроек
	Выбор баз данных для контроля целостности, выбор модулей баз данных.	Выбор баз данных и модулей
		Сохранение результатов настроек
Ограничение прав пользователей по вводу информации в информационную систему	Выбор объектов файловой системы, объектов баз данных, объектов прикладного и специального программного обеспечения	Импорт объектов из журнала регистрации событий
		Сохранение результатов настройки

Диаграмма прецедентов подсистемы настройки идентификации и аутентификации представлена на рисунке 38.

Диаграмма прецедентов подсистемы настройки управления доступом представлена на рисунке 39.

Диаграмма прецедентов подсистемы настройки ЗПС представлена на рисунке 40.

Диаграмма прецедентов подсистемы настройки управления носителями информации представлена на рисунке 41.

Диаграмма прецедентов подсистемы настройки регистрации и учета представлена на рисунке 42.

Диаграмма прецедентов подсистемы настройки контроля целостности представлена на рисунке 43.

Синим цветом обозначены высокоуровневые требования. Красным цветом обозначены низкоуровневые требования. Зеленым цветом обозначены дополнительные требования.



Рисунок 38 - Диаграмма прецедентов подсистемы настройки идентификации и аутентификации



Рисунок 39 - Диаграмма прецедентов подсистемы настройки управления доступом

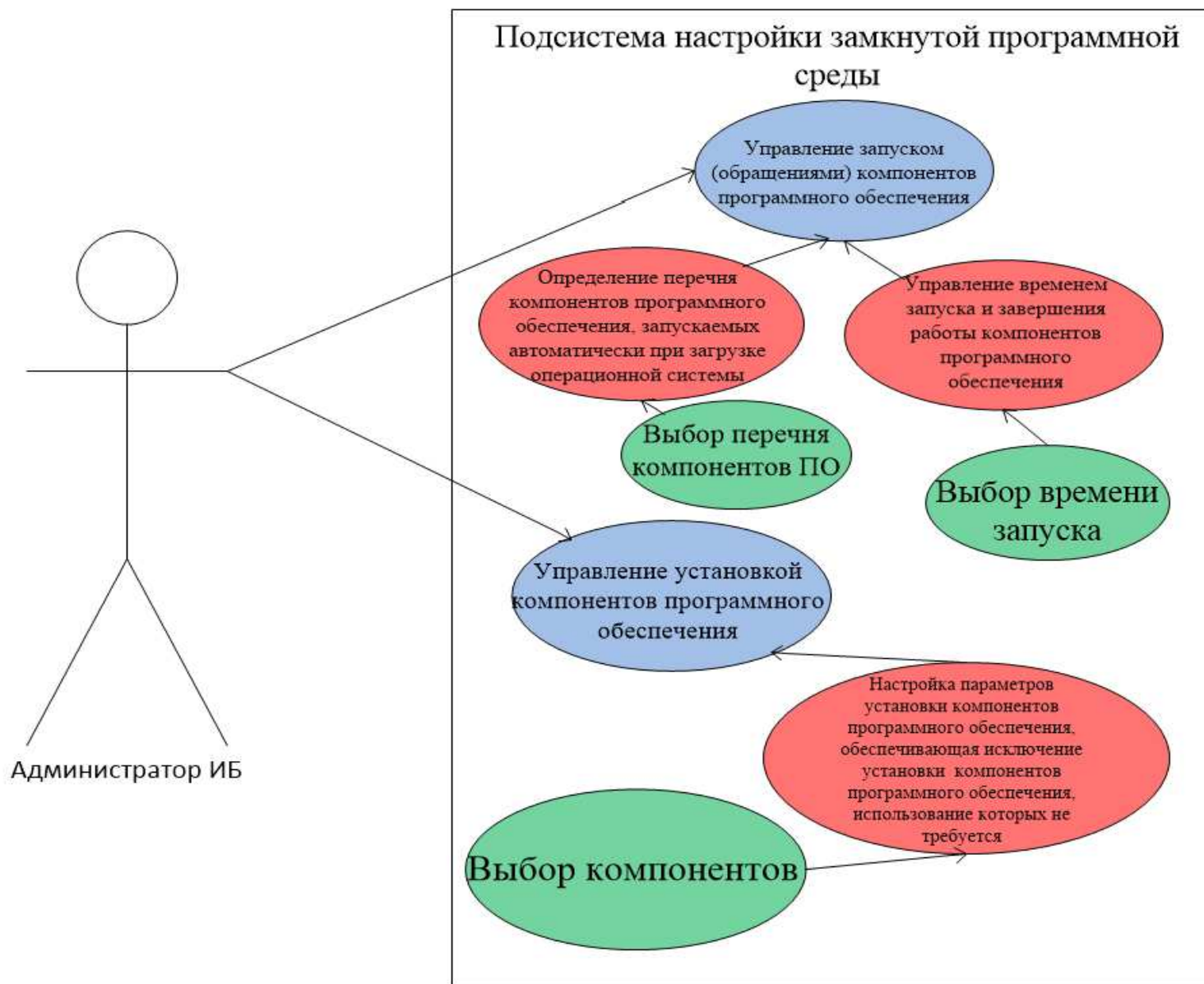


Рисунок 40 - Диаграмма прецедентов подсистемы настройки ЗПС

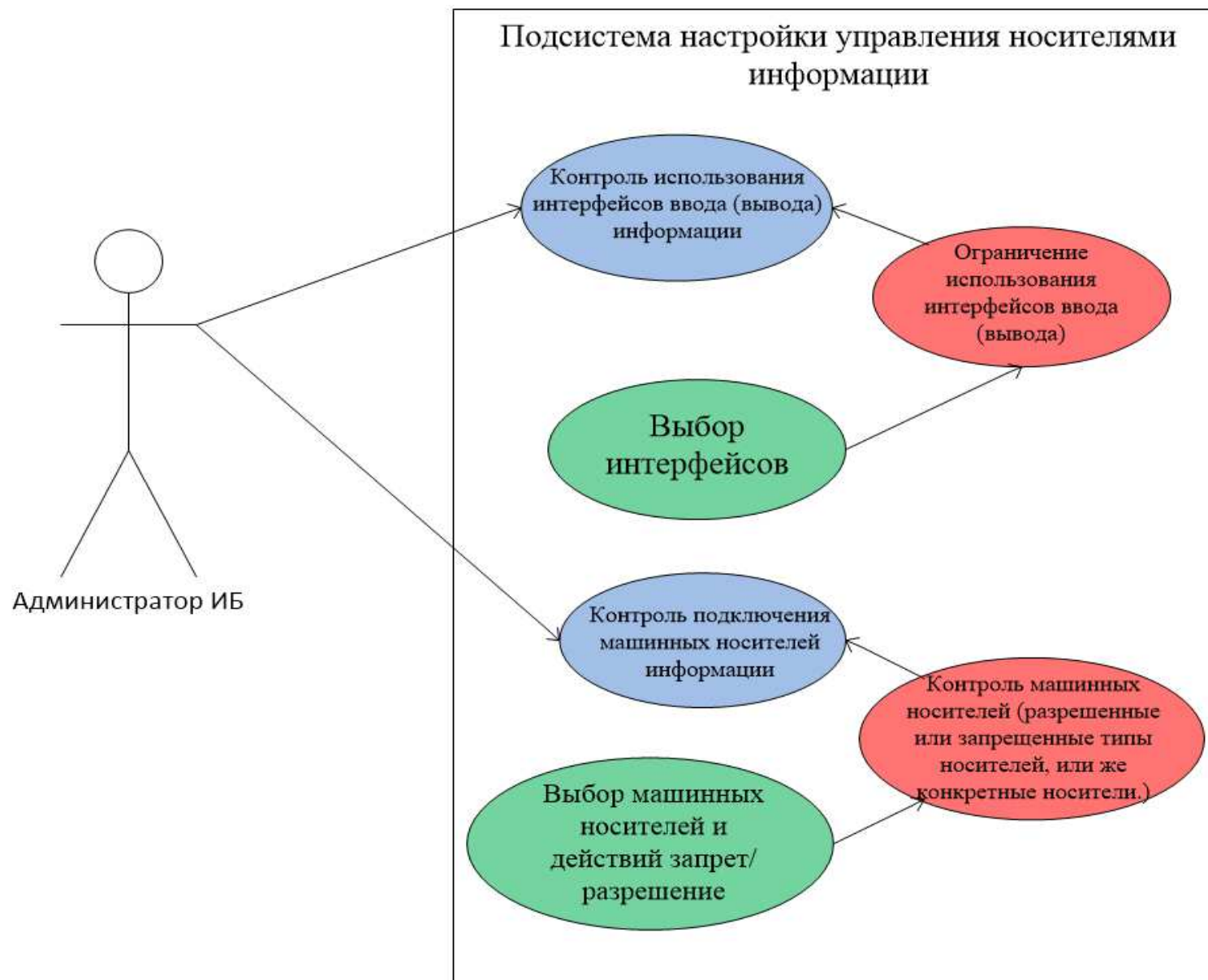


Рисунок 41 - Диаграмма прецедентов подсистемы настройки управления носителями информации

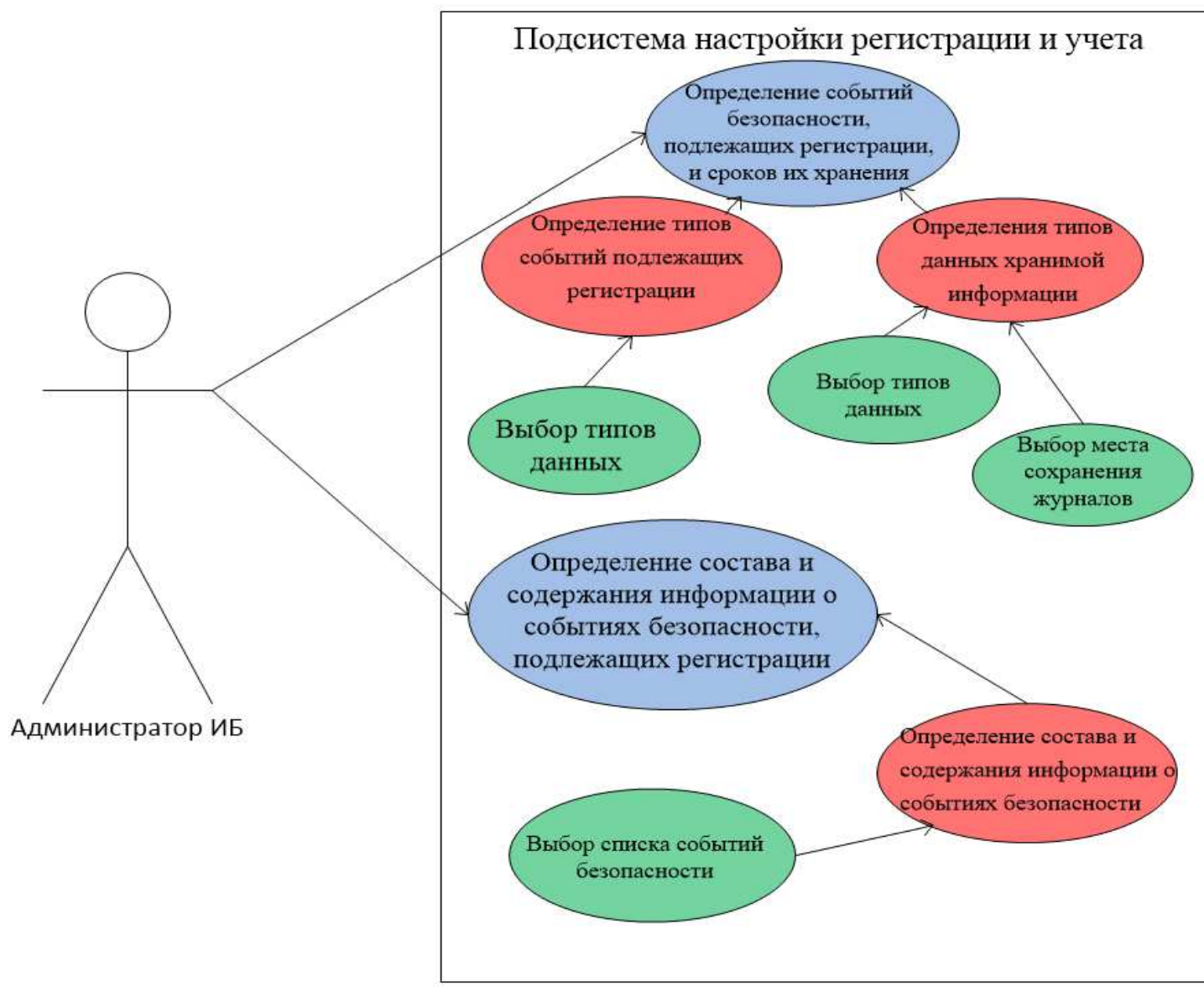


Рисунок 42 - Диаграмма прецедентов подсистемы настройки регистрации и учета

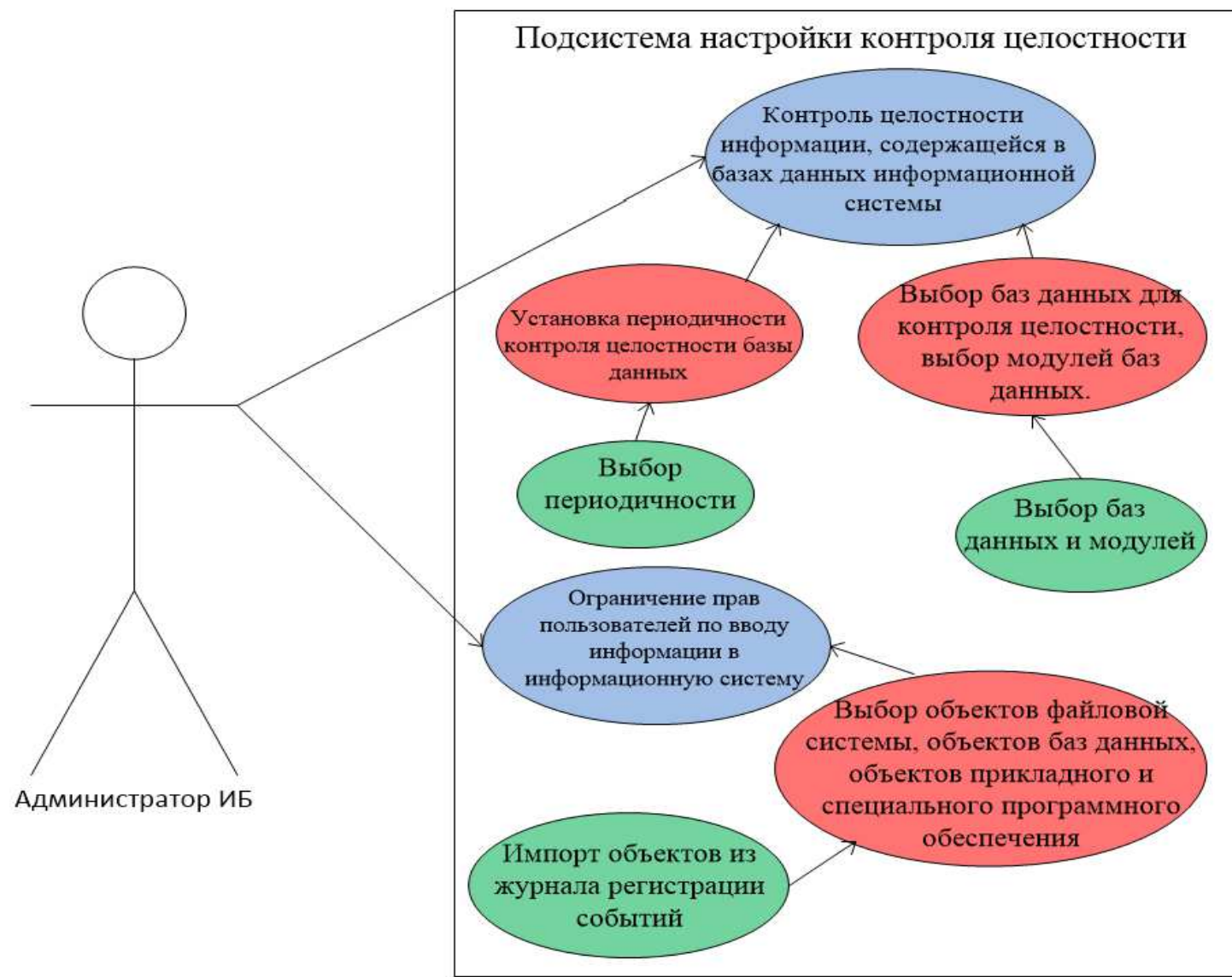


Рисунок 43 - Диаграмма прецедентов подсистемы настройки контроля целостности

8 Проектирование типовых элементов пользовательского интерфейса подсистемы настройки средства защиты информации от несанкционированного доступа.

8.1 Методы повышения удобства пользовательского интерфейса подсистемы настройки средства защиты информации от несанкционированного доступа при использовании мировых практик

В данном разделе осуществляется разработка типовых пользовательских элементов пользовательского интерфейса. Стоит отметить, что удобство использования данной подсистемы настройки оценивается весьма субъективно, и этот раздел не является обязательным требованием, так как визуализация подсистемы настройки СЗИ от НСД в полной мере зависит от желаний разработчика. При проектировании типовых элементов подсистемы настройки СЗИ от НСД необходимо повысить удобство пользовательского интерфейса путем введения дополнительных функций.

Не смотря на субъективность восприятия интерфейса подсистемы настройки, следует определить несколько критериев, позволяющих улучшить пользовательский интерфейс:

- лучше тот интерфейс, при котором время выполнения задачи меньше;
- лучше тот интерфейс, в котором число произвольных ошибок пользователя меньше;
- неоднозначность в восприятии интерфейса должна быть минимальна (это способствует самообучению пользователей);
- объем вводимой пользователем информации должен стремиться к минимуму (одни и те же данные не должны вводиться несколько раз)
- простота и визуальная привлекательность (удобство использования не менее важно, чем функциональность).

8.2 Подсистема настройки идентификации и аутентификации

Первым требованием является «Формирование идентификатора пользователя или устройства» для реализации данного требования необходимо создать настройку конкретного пользователя, предоставить возможность инициализировать электронный идентификатор, также управление идентификатором, задать возможность записать пароль в идентификатор или записать идентификатор в закрытый ключ пользователя. Результаты визуализации представлены на рисунке 44.

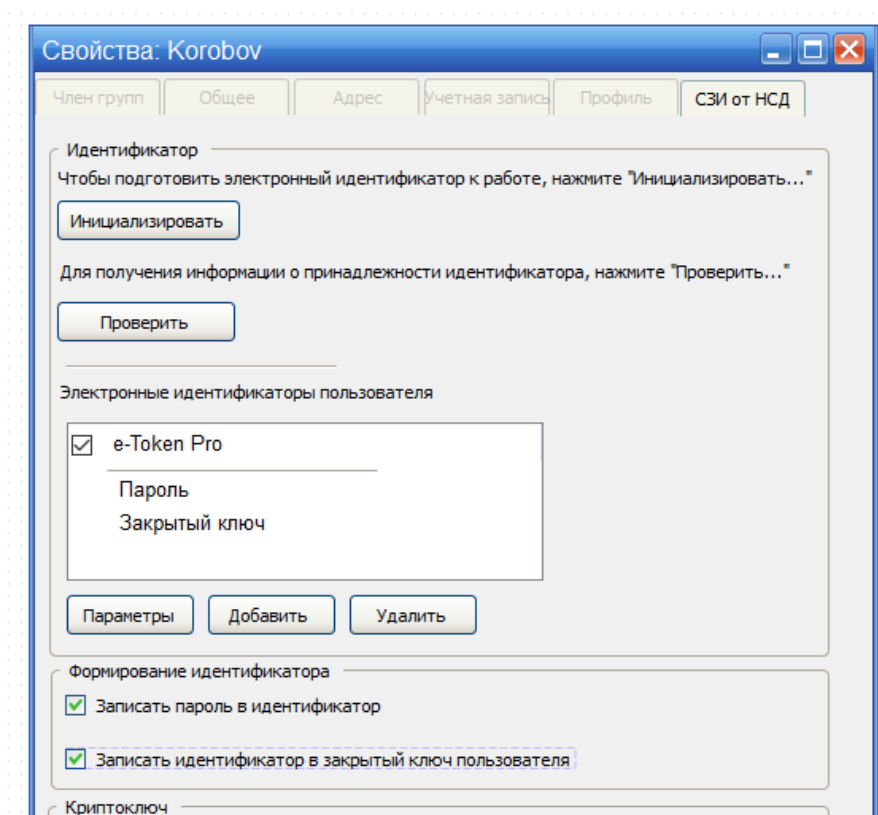
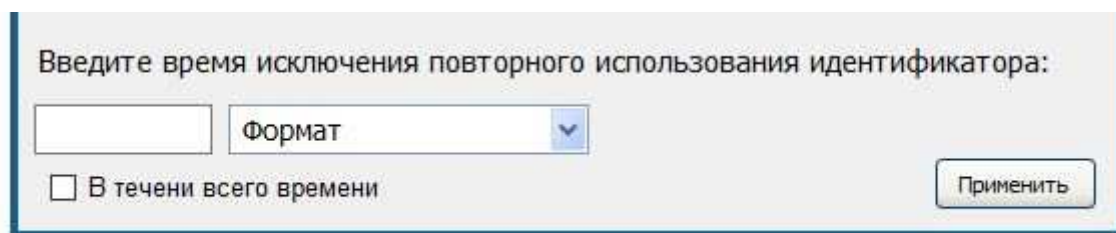


Рисунок 44 - Интерфейс формирования идентификатора

Следующим требованием является «Исключение повторного использования идентификатора». В данной функции необходимо реализовать поле, где будет задаваться значение времени исключения повторного использования идентификатора. Также необходимо реализовать функцию выбора формата времени (дней, месяцев, лет) путем выпадения диалогового окна. Однако согласно требованиям ФСТЭК должна быть функция исключения

повторного использования в течении всего времени эксплуатации ИС А также необходимо реализовать функцию сохранения данной настройки. Результаты представлены на рисунке 45.



Введите время исключения повторного использования идентификатора:

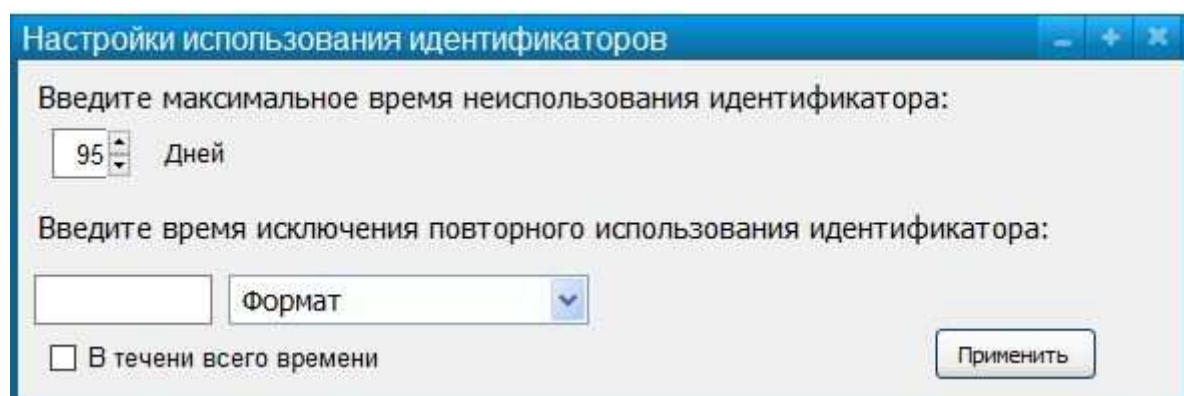
Формат

☐ В течени всего времени

Применить

Рисунок 45 - Интерфейс исключения повторного использования идентификатора

Следующее требование «Блокирование идентификатора пользователя через период времени неиспользования». Необходимо задать временные значения блокирования идентификатора. Согласно требованию ФСТЭК срок должен не превышать 95 дней. Так как настройка «Исключение повторного использования идентификатора». Находится в том же окне «Настройки использования идентификаторов», то кнопка сохраняющая результат у них общая. Результат работы представлен на рисунке 46.



Настройки использования идентификаторов

Введите максимальное время неиспользования идентификатора:

95 Дней

Введите время исключения повторного использования идентификатора:

Формат

☐ В течени всего времени

Применить

Рисунок 46 - Блокирование идентификатора пользователя через период времени неиспользования

Следующее требование «Изменение аутентификационной информации», где согласно требованию ФСТЭК необходимо создать и изменить аутентификационную информацию. Соответственно необходимо реализовать

функцию присвоения криптоключа пользователю. Данная функция находится в настройках пользователя. Также реализовать функцию изменения пароля и необходимо реализовать функцию сохранения данных настроек. Изменить пароль пользователя можно перейдя по ссылке в настройках пользователя. Результаты представлены на рисунке 47.

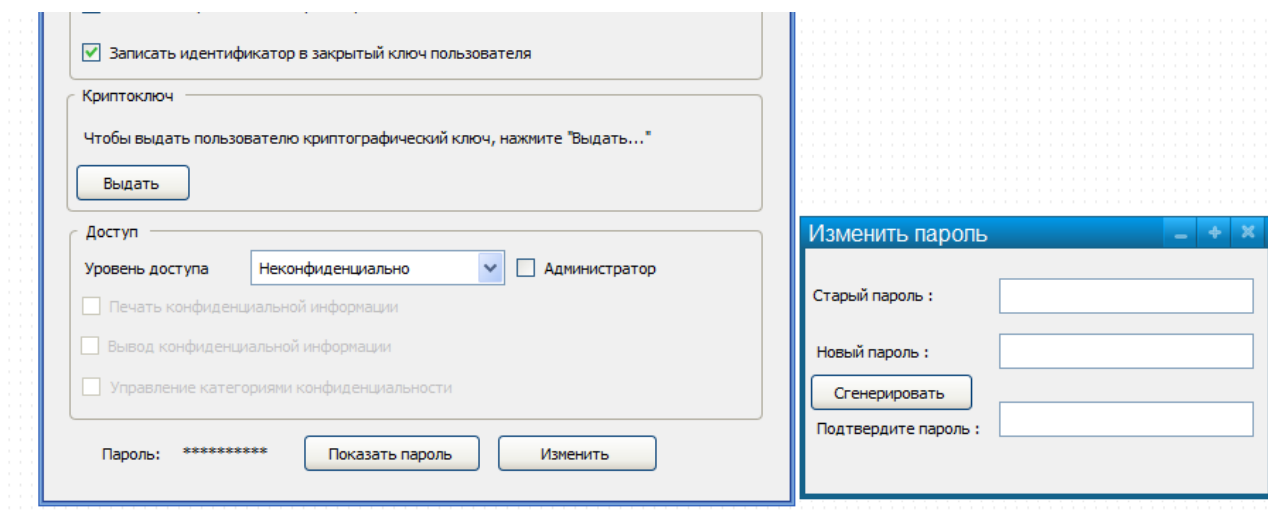


Рисунок 47 - Интерфейс изменения аутентификационной информации

Следующее требование «Изменение характеристик пароля». В окне конфигурации пароля, необходимо реализовать группу изменения характеристик пароля. Куда входит выбор длины пароля(не менее 6 символов), выбор неуспешных попыток ввода пароля (минимальное значение 3). Также можно в данном окне реализовать требование «Установка времени блокировки в случае неуспешного ввода», для реализации нужно создать окно ввода времени блокировки (минимальное значение согласно требованиям 3 минуты). «Выбор алфавита пароля» также реализовано в настройках пароля. А также требование «Установка промежутка времени на смену пароля» с окном выбора промежутка времени после блокирования (согласно требованиям не более 180 дней). Результаты представлены на рисунке 48.

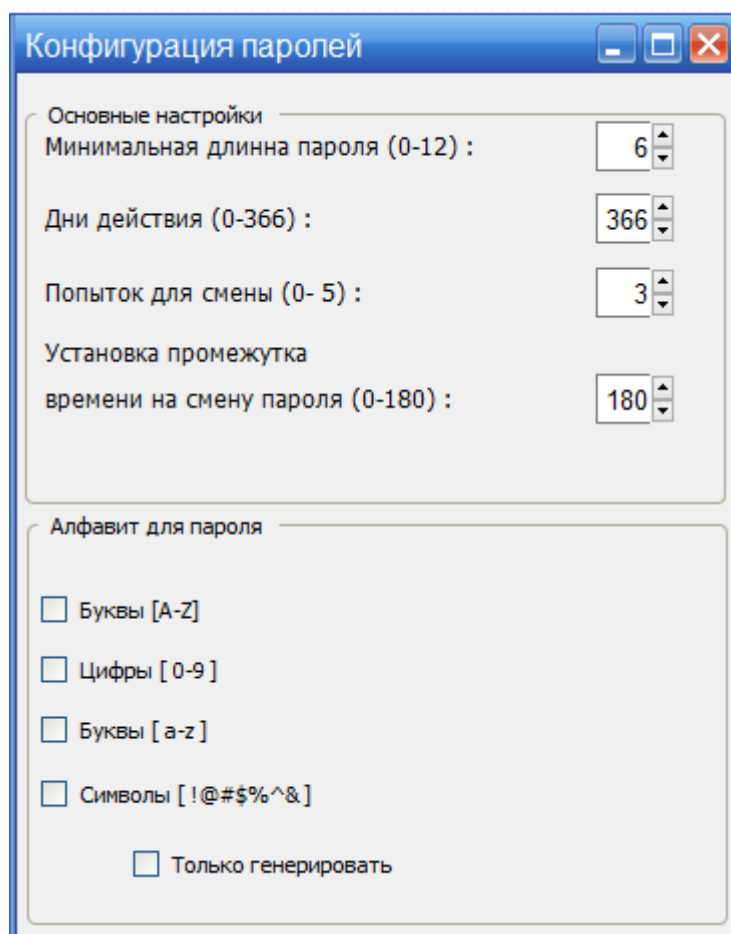


Рисунок 48 - Интерфейс конфигурация паролей

8.3 Подсистема настройки управления доступом

Следующее требование «Определение типа учетной записи» Необходимо создать окно где будет определяться пользователь (внутренний пользователь, внешний пользователь, гость, временная учетная запись и предоставить возможность создавать свои типы пользователей) и сопоставляться тип учетной записи. Данную функцию также можно реализовать при создании пользователя. Но целесообразно внедрить данную функцию в настройки пользователя. Если нажать кнопку выбрать откроется окно со списком всех пользователей. Результат представлен на рисунке 49.

Рисунок 49 - Определение типа учетной записи

Следующее требование «Группирование учетных записей», данную функцию можно реализовать с помощью функции «Настройка групп». Необходимо создать окно выбора определенной группы. Также добавить возможность создавать группы самому. После чего нажать клавишу «Выбрать пользователя», где появится окно с учетными записями пользователей, а также группа к которой данный пользователь принадлежит. Также можно данную функцию реализовать в самой настройке учетной записи. Результаты представлены на рисунке 50.

Рисунок 50 - Группирование учетных записей

Далее требование «Заведение, активация, блокирование и уничтожение учетных записей пользователей.». Данное требование необходимо реализовать

в настройках учетных записей. В данную настройку можно применить требование «Корректировка учетных записей». Результат представлен на рисунке 51.

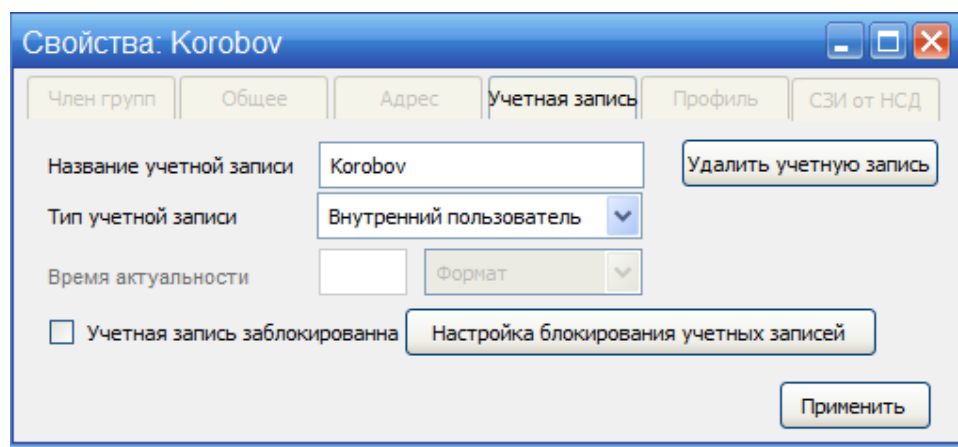


Рисунок 51 - Интерфейс настройки учетной записи

Следующие требования «Определение срока актуальности временной учетной записи» Можно реализовать окном выбора срока актуальности временной учетной записи. Срок актуальности необходимо реализовать как в настройках самого пользователя, так и в общих настройках. Результат представлен на рисунке 52

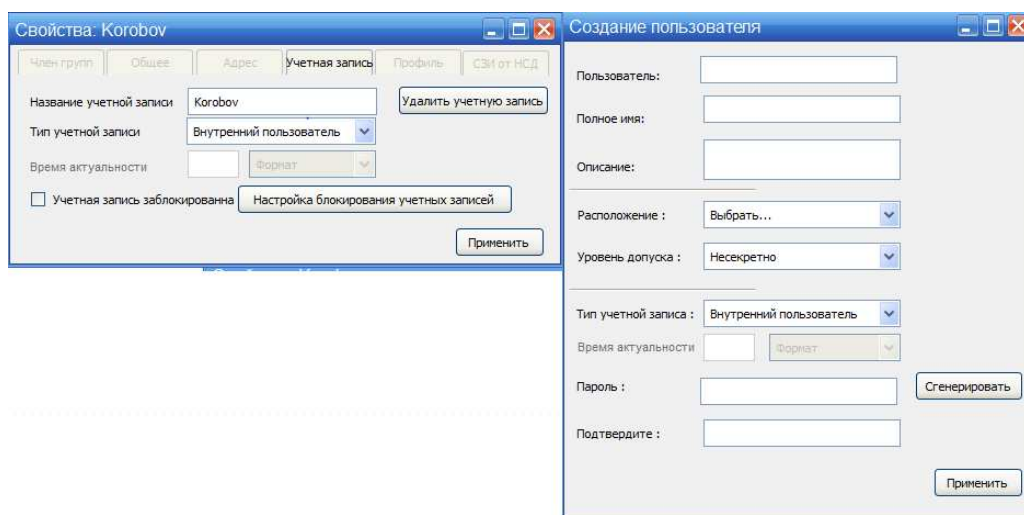


Рисунок 52 - Определение срока актуальности временной учетной записи

Следующие требования «Автоматическое блокирование неиспользуемых учетных записей» (максимальный срок согласно требованиям 95 дней), «Блокирования учетных записей»(выбор количества неуспешной

аутентификации), «Ограничение неуспешных попыток входа в информационную систему», «Определение времени бездействия пользователя» объединены в настройку учетных записей. Для определения максимального срока блокирования неиспользуемых учетных записей, необходимо настроить кнопку перехода в настройки идентификаторов. Для установки числа неуспешных попыток аутентификации необходимо перейти в конфигурации пароля. Также реализована функция интеграции событий безопасности с настройки подсистемы регистрации и учета. Можно выбрать события безопасности в ручную. Результат приведен на рисунке 53.

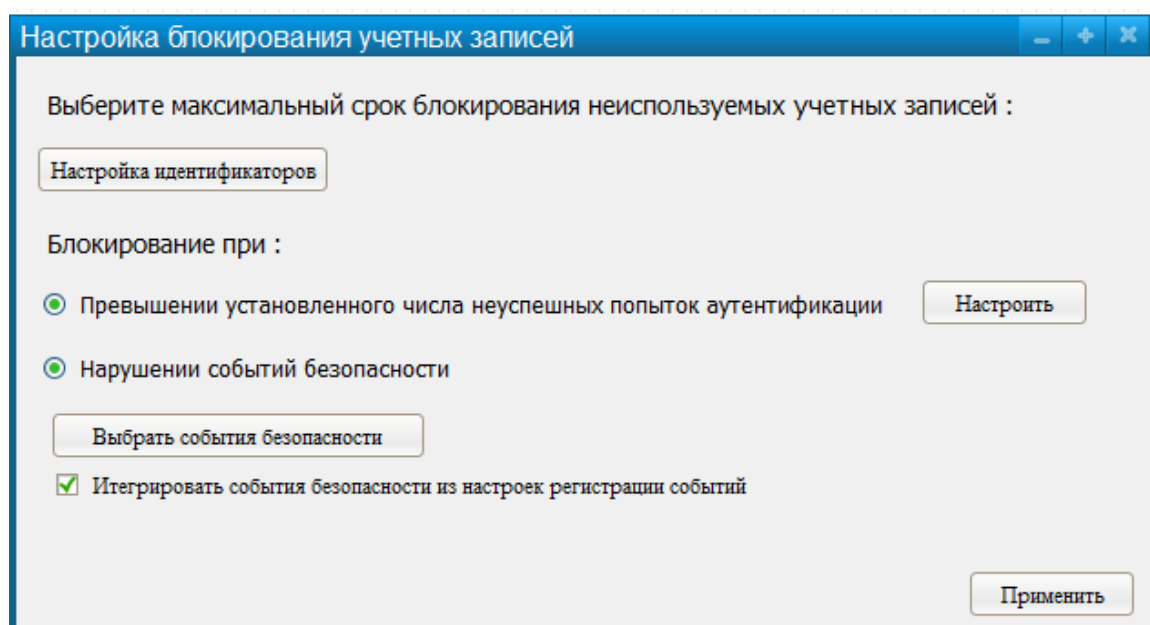


Рисунок 53 - Настройка блокирования учетных записей

Следующие требования «Разграничение ролей (администрирование, мониторинг, обработка информации)», «Предоставление прав к функциям безопасности», «Обновление, назначение, изменение и сохранение атрибутов безопасности (меток безопасности)», «Регламентация мобильных технических средств», «Контроль мобильных технических средств» реализуются в окне разграничения доступа. Также есть переход к настройкам мандатного и дескреционного доступа. Результаты приведены на рисунке 54.

Рисунок 54 - Настройки разграничения доступа

Следующим требованием является «Дискреционный метод разграничения». Проблема дискреционного разграничения заключается в том, что используется большой массив объектов и субъектов доступа. Необходимо осуществить импорт групп пользователей, импорт типов пользователей, также реализовать импорт настроек подсистемы регистрации, и предоставить возможность использовать настройки из шаблона. Также необходимо реализовать кнопку перехода к матрице доступа. Результаты представлены на рисунке 55.

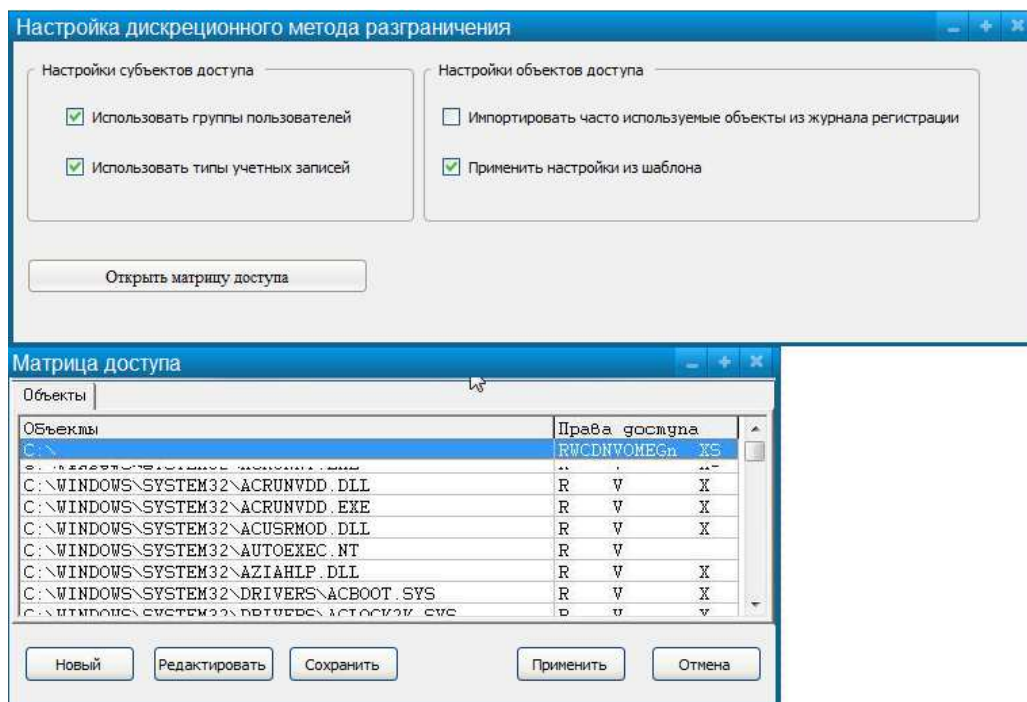


Рисунок 56 - Настройка матрицы доступа

Следующим требованием является «Мандатный метод разграничения», необходимо реализовать функцию пользователей, групп пользователей, а также разрешенные действия к объекту. Также необходимо задать функцию задания атрибутов мандатного разграничения доступа. Результат представлен на рисунке 57.

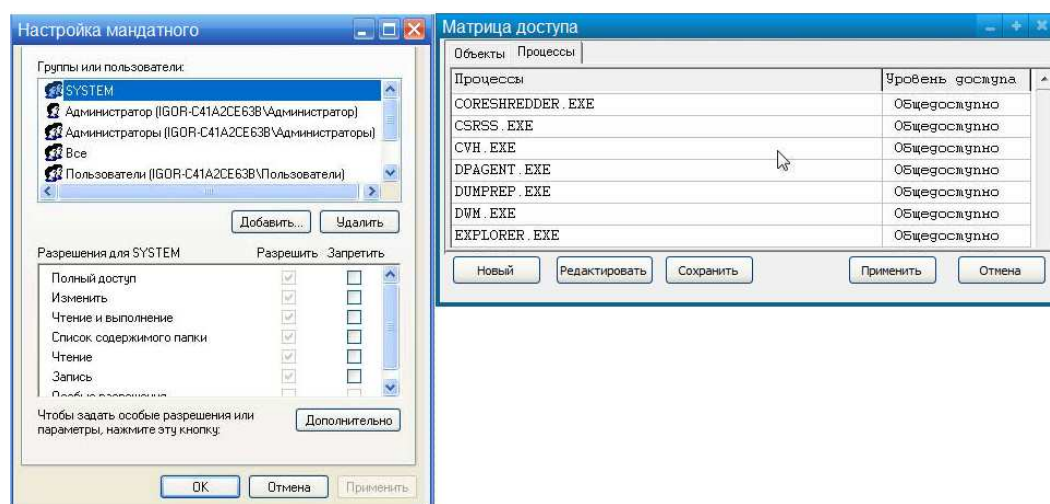


Рисунок 57 - Мандатное разграничение доступа

Следующее требование «Определение компонентов доверенной загрузки», необходимо предоставить возможность выбрать компоненты доверенной загрузки, а также предоставить возможность экспортировать настройки из шаблона. Настройка доверенной загрузки осуществляется через BIOS.

8.4 Подсистема настройки замкнутой программной среды

Первым требованием является «Определение перечня компонентов программного обеспечения, запускаемых автоматически при загрузке операционной системы» для реализации данного требования, необходимо задать функцию выбора перечня компонентов ПО. Также в окне настройки ЗПС можно реализовать требование «Управление временем запуска и завершения работы компонентов программного обеспечения» необходима функция , где будут задаваться временные значения запуска и завершения. Также необходимо реализовать функцию «Настройка параметров установки компонентов программного обеспечения, обеспечивающая исключение установки (если осуществимо) компонентов программного обеспечения, использование которых не требуется» Необходимо реализовать функцию предоставляющую выбор компонентов программного обеспечения. Результаты представлены на рисунке 58.

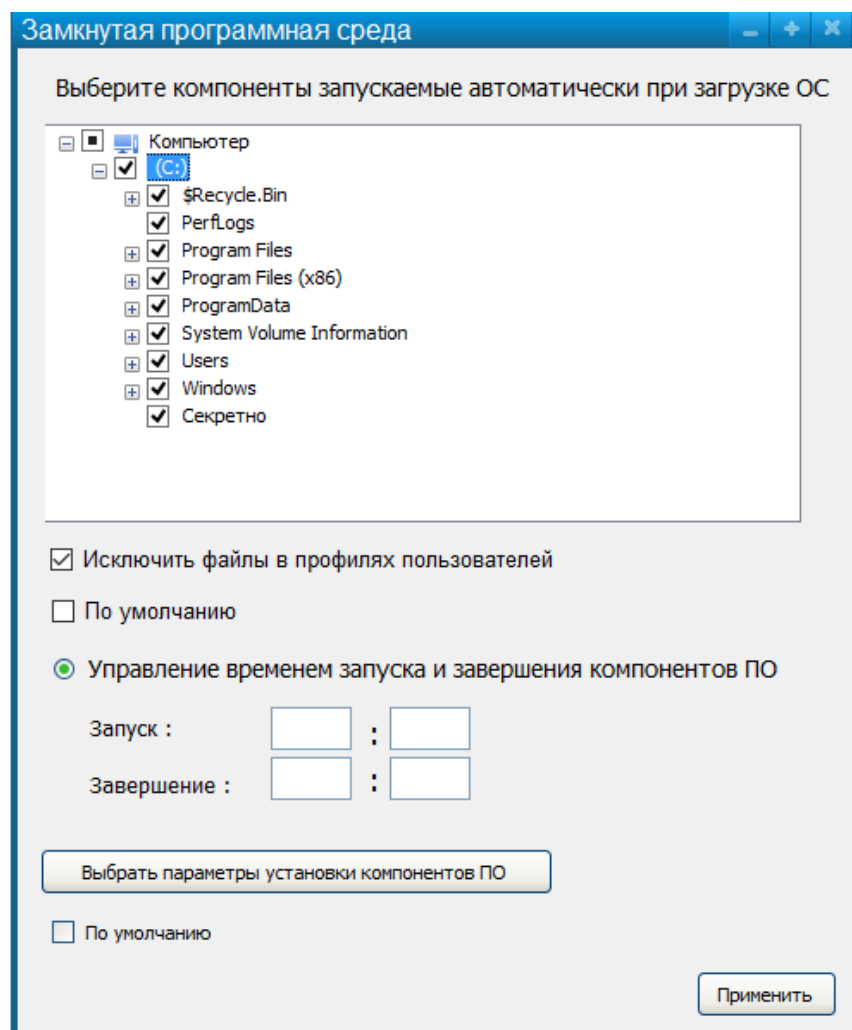


Рисунок 58 - Интерфейс настройки ЗПС.

8.5 Подсистема настройки управления носителями информации

Требования «Ограничение использования интерфейсов ввода (вывода)» и «Контроль машинных носителей (разрешенные или запрещенные типы носителей, или же конкретные носители.)» можно реализовать путем окна выбора данных интерфейсов/носителей, также необходимо выбрать пользователя которому будет применяться настройки, групп пользователей, ролей и типов пользователей. разрешенные интерфейсы необходимо поставить галочку. Результат работы приведен на рисунке 59.

Настройка управления носителями

Название: Nositel1
Серийный номер: 6a41d6d2

Учётный номер: 024
Пользователь: Korobov
Гриф: Секретно
Дата: 01.09.2015 15:36:55
Тип подключения: Usb
Дополнительный аудит: Не выполнять
Примечание:

☒ Использовать простой доступ к носителю
☐ Использовать преобразование информации
☐ Проверять разрешения для папки при доступе к вложенным объектам

Настройка интерфейсов ввода (вывода)

Применить

Рисунок 59 - Интерфейс настройки управления носителями информации

8.6 Подсистема настройки регистрации и учета

Следующим требованием является «Определение типов событий подлежащих регистрации». Данное требование можно реализовать путем выбора типов данных регистрации событий. Требование «Определения типов данных хранимой информации». Данное требование можно реализовать путем выбора сохранения информации (Все записи журнала, события безопасности). Требование «Определение состава и содержания информации о событиях безопасности» Результат представлен на рисунке 60.

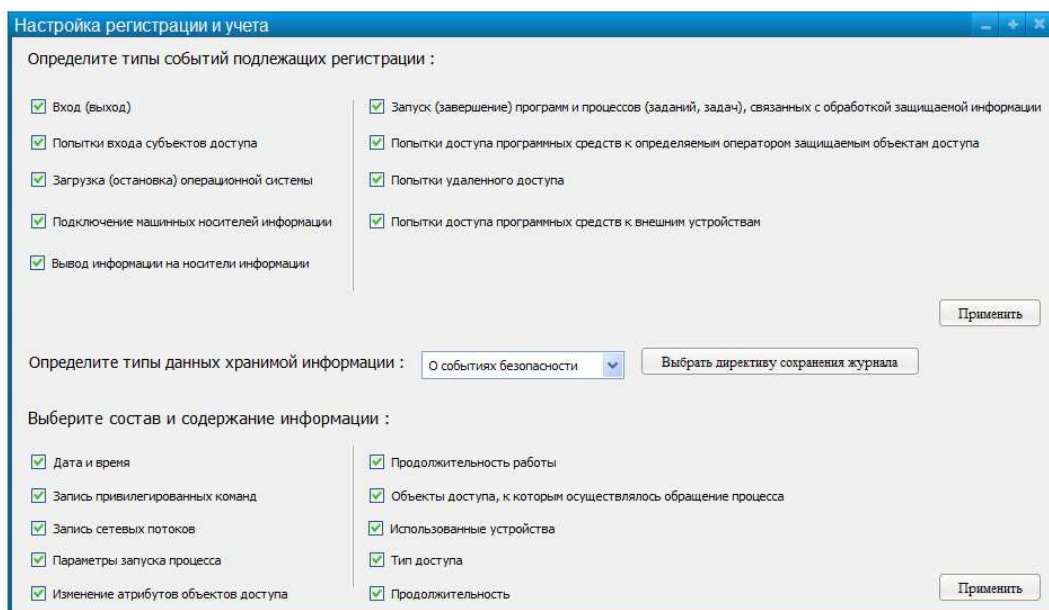


Рисунок 60 - Интерфейс настройки регистрации и учета

8.7 Подсистема настройки контроля целостности

Следующим требованием является «Установка периодичности контроля целостности базы данных» необходимо реализовать окно выбора периодичности контроля целостности баз данных. «Выбор баз данных для контроля целостности, выбор модулей баз данных». Для реализации данного требования необходимо реализовать выпадающее окно баз данных используемых в системе и выбрать конкретную базу данных. Также существует требование «Выбор объектов файловой системы, объектов баз данных, объектов прикладного и специального программного обеспечения», данные объекты можно выбрать как в ручную, так и экспортировать объекты из журнала регистрации событий. Результаты представлены на рисунке 61.

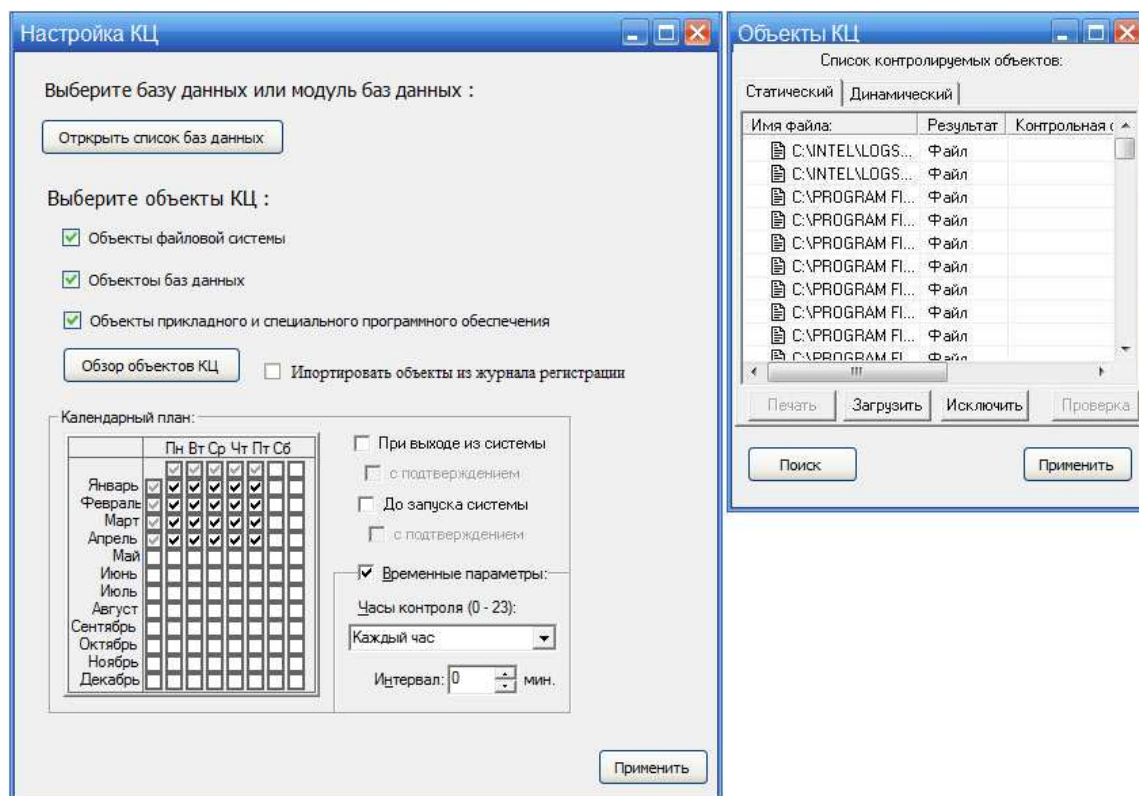


Рисунок 61 - Интерфейс настройки КЦ

ЗАКЛЮЧЕНИЕ

Целью дипломного проекта является разработка подсистемы настройки СЗИ от НСД, отвечающей требованиям полноты функционала и удобства использования.

В результате достижения поставленной цели была поставлена проблема проектирования подсистемы настройки СЗИ от НСД, а также разработаны требования к подсистеме настройки СЗИ от НСД и спроектирована подсистема настройки СЗИ от НСД.

В рамках постановки проблем проектирования подсистемы настройки СЗИ от НСД был проведен анализ факторов, определяющих требования к подсистеме настройки средств защиты информации, осуществлено исследование подсистем настройки в существующих СЗИ, выявлены сложности, связанные с проектированием подсистем настройки СЗИ.

В рамках разработки требований к подсистеме настройки СЗИ от НСД был проведен анализ технических требований по обеспечению информационной безопасности информационных систем, содержащихся в отечественных нормативно-методических документах, осуществлена классификация технических требований в зависимости от степени и характера влияния на компоненты подсистемы настройки СЗИ от НСД, осуществлено формирование комплекса требований к подсистеме настройки СЗИ от НСД.

В рамках проектирования подсистемы настройки СЗИ от НСД было осуществлено проектирование компонентов подсистемы настройки СЗИ от НСД, проектирование интерфейсов взаимодействия компонентов подсистемы настройки с другими подсистемами СЗИ от НСД, проектирование типовых элементов пользовательского интерфейса подсистемы настройки средства защиты информации от несанкционированного доступа.

Соответственно работа была выполнена в полном объеме в соответствии с техническим заданием на выпускную квалификационную работу.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Герасимов А.А., Кузнецов В.А., Мозговой А.В, Пугачев К.А. Основные подсистемы защиты информации от несанкционированного доступа и особенности их настройки. М.: МГТУ им. Н.Э. Баумана, 2013 - 4 с.
2. СЗИ «Страж NT» Руководство администратора// ООО «РУБИНТЕХ», 2016 URL: http://www.guardnt.ru/download/doc/admin_guide_nt_4_0.pdf (дата обращения: 10.09.2016).
3. Secret Net 7 Руководство администратора. Настройка механизмов защиты // ООО «Код Безопасности», 2016. URL: http://www.securitycode.ru/_upload/editor_files/documentation/sobol_2//7/Secret_Net_Admin_Guide_Security_Settings.pdf (дата обращения: 10.09.2016).
4. Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа «АККОРД-Win64» (версия 4.0) «РУКОВОДСТВО АДМИНИСТРАТОРА» // ЗАО ОКБ «САПР», 2010. URL: www.accord.ru/docs/awin64/Administrator_Guide.pdf (дата обращения: 10.09.2016).
5. «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» приказ ФСТЭК России N 17 от 11 февраля 2013 г.;
6. «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» приказ ФСТЭК России N 21 18 февраля 2013 г.;
7. «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования» приказ ФСТЭК России N 489 от 31 августа 2010 г.;
8. «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и

технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» приказ ФСТЭК России N 31 от 14 марта 2014г.;

9. «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» руководящий документ ФСТЭК. Решение председателя Гостехкомиссии России от 30 марта 1992 г.;

10. «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» руководящий документ ФСТЭК. Решение председателя Гостехкомиссии России от 30 марта 1992 г.;

11. «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации» руководящий документ ФСТЭК. Решение председателя Гостехкомиссии России от 30 марта 1992 г.;

12. Меры защиты информации в государственных информационных системах/ методический документ, ФСТЭК, 2014г.

ПРИЛОЖЕНИЕ А