|  |
| --- |
|  |
|  |
|  |
|  |

**Сиcтема контроля прав доступа**

**«Матрица доступа»**

**Описание применения**

**Лист утверждения**

58.29.29-001-29233469-2020 31 01 – ЛУ

2020

|  |  |
| --- | --- |
| **УТВЕРЖДЕН** |  |
| 58.29.29-001-29233469-2020 31 01 –ЛУ |  |

**Сиcтема контроля прав доступа**

**«Матрица доступа»**

**Описание** **применения**

58.29.29-001-29233469-2020 31 01

На 16 листах

2020

АННОТАЦИЯ

В данном программном документе приведено описание программного средства контроля (анализа) защищенности информации «Система контроля прав доступа «Матрица доступа»», децимальный номер 58.29.29-001-29233469-2020, (далее – Система).

В разделе «Назначение Системы» приведено описание назначения Системы, ее возможности, основные характеристики, а также ограничения, накладываемые на область применения Системы.

В разделе «Условия применения» указаны условия, необходимые для функционирования Системы: требования к необходимым для Системы техническим средствам, программам, общие характеристики входной и выходной информации, а также требования и условия организационного, технического и технологического характера.

В разделе «Описание задачи» указаны задачи, решаемые Системой, методы их решения.

В разделе «Входные и выходные данные» указаны сведения о входных и выходных данных Системы.

СОДЕРЖАНИЕ

[1. Назначение Системы 4](#_Toc52802098)

[1.1. Назначение Системы 4](#_Toc52802099)

[1.2. Возможности Системы 5](#_Toc52802100)

[1.2.1. Контроль заведения и удаления учетных записей пользователей в защищаемой системе – службе каталогов MS Active Directory 5](#_Toc52802101)

[1.2.2. Контроль реализации правил разграничения доступом 6](#_Toc52802102)

[1.2.3. Контроль реализации полномочий пользователей 6](#_Toc52802103)

[1.3. Ограничения, накладываемые на область применения Системы 6](#_Toc52802104)

[2. Условия применения 7](#_Toc52802105)

[2.1. Требования к аппаратному и программному обеспечению 7](#_Toc52802106)

[2.2. Общие характеристики входной и выходной информации 7](#_Toc52802107)

[2.3. Требования и условия организационного характера 8](#_Toc52802108)

[2.4. Требования и условия технического характера 9](#_Toc52802109)

[2.5. Требования и условия технологического характера 9](#_Toc52802110)

[3. Описание задачи 10](#_Toc52802111)

[3.1. Определение задачи 10](#_Toc52802112)

[3.2. Метод решения задачи 10](#_Toc52802113)

[3.2.1. Контроль заведения и удаления учетных записей пользователей 10](#_Toc52802114)

[3.2.2. Контроль реализации правил разграничения доступом 10](#_Toc52802115)

[3.2.3. Контроль реализации полномочий пользователей 10](#_Toc52802116)

[4. Входные и выходные данные 12](#_Toc52802117)

[Перечень терминов 13](#_Toc52802118)

[Перечень сокращений 14](#_Toc52802119)

# Назначение Системы

## Назначение Системы

Система предназначена для контроля реализации правил разграничения доступом и формирования актуальной матрицы прав доступа пользователей к корпоративным информационным ресурсам/системам (далее – Защищаемые системы), а также выявления произошедших изменений в правах доступа. Подключение Системы к защищаемым системам осуществляется посредством программных коннекторов с использованием встроенных механизмов (API-функции, процедуры и т.д.) данных систем. Реализация программных коннекторов не предполагает установки дополнительных программных компонентов на серверы защищаемых систем.

Система является программным средством контроля (анализа) защищенности информации, реализующим меру защиты информации «Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе» (АНЗ.5) в соответствии с требованиями документов «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (введены в действие приказом ФСТЭК России № 17 от 11.02.2013), «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (введены в действие приказом ФСТЭК России № 21 от 18.02.2013) и «Меры защиты информации в государственных информационных системах» (утверждены директором ФСТЭК России 11.02.2014), в части:

* контроль заведения и удаления учетных записей пользователей,
* контроль реализации правил разграничения доступом,
* контроль реализации полномочий пользователей.

Общая схема архитектуры Системы представлена на рисунке ниже (Рис. 1).

**Структурная схема Системы**



Рис.

Управление Системой осуществляется с АРМ администратора посредством веб-консоли управления.

ПО, обеспечивающее выполнение функциональных возможностей Системы, устанавливается на сервер приложений. Программные коннекторы для подключения к защищаемым системам также устанавливаются на сервер приложений.

Хранение конфигурационных параметров Системы, а также хранение сформированных матриц текущих прав доступа для защищаемых систем осуществляется на сервере баз данных.

## Возможности Системы

Система предназначена для решения следующих задач.

### Контроль заведения и удаления учетных записей пользователей в защищаемой системе – службе каталогов MS Active Directory

Система предоставляет возможность контроля заведения и удаления учетных записей пользователей в защищаемой системе – службе каталогов MS Active Directory. Это обеспечивается реализацией следующих функциональных возможностей:

1. построение матрицы вхождения пользователей в группы безопасности службы каталогов MS Active Directory;
2. возможность контекстного поиска записей в сформированной матрице по пользователям и группам безопасности службы каталогов MS Active Directory;
3. возможность сохранения сформированной матрицы в качестве эталона;
4. сравнение сформированной матрицы текущих прав доступа пользователей защищаемой системы с эталоном и отображение выявленных изменений.

### Контроль реализации правил разграничения доступом

Система предоставляет возможность контроля реализации правил разграничения доступом в защищаемой системе с дискреционной либо ролевой моделями управления доступом. Это обеспечивается посредством построения матрицы текущих прав доступа пользователей в защищаемой системе с дискреционной либо ролевой моделями управления доступом.

### Контроль реализации полномочий пользователей

Система предоставляет возможность контроля реализации полномочий пользователей в защищаемой системе. Это обеспечивается реализацией следующих функциональных возможностей:

1. возможность контекстного поиска записей в сформированной матрице доступа по объектам доступа защищаемой системы;
2. отображение текущих прав доступа для заданного пользователя защищаемой системы с дискреционной либо ролевой моделями управления доступом;
3. возможность сохранения сформированной матрицы текущих прав доступа пользователей в качестве эталона;
4. сравнение сформированной матрицы текущих прав доступа пользователей защищаемой системы с эталоном и отображение выявленных изменений;
5. ведение истории прав доступа.

## Ограничения, накладываемые на область применения Системы

Система не предназначена для обработки сведений, содержащих государственную тайну.

# Условия применения

## Требования к аппаратному и программному обеспечению

Требования к аппаратному и программному обеспечению описаны в таблице ниже (Таблица 2.1).

Таблица . - Требования к аппаратному и программному обеспечению

| **Компонент Системы** | **Требования  к аппаратной части** | **Требования к программной части** |
| --- | --- | --- |
| ПО «Система контроля прав доступа «Матрица доступа»» и СУБД | * процессор: 2 или более ядер с частотой 2.4 ГГц; * оперативная память: 8 ГБ; * свободное дисковое пространство: не менее 150 ГБ | 1. Операционная система:  * Windows Server 2008 R2 Standard * Windows Server 2008 R2 Enterprise * Windows Server 2012 Standard * Windows Server 2012 R2 Standard * Windows Server 2016 Standard * Windows Server 2019 Standard  1. Python версии 3.8.1; 2. Веб сервер Apache HTTP Server версии 2.4 3. СУБД PostgreSQL версии 10.3-2 4. Распространяемый пакет Visual C++ для Visual Studio 2013   Распространяемый пакет Visual C++ для Visual Studio 2017 |

## Общие характеристики входной и выходной информации

Входными данными Системы являются:

1. данные о субъектах информационных систем;
2. данные о структуре объектов доступа;
3. данные о правах доступа пользователей информационных систем;
4. данные для настроек подключения к информационным ресурсам.

Выходными данными Системы являются матрицы прав доступа информационных систем, а так же матрицы вхождения пользователей в группы, хранящиеся в БД и представляющиеся в веб-интерфейсе.

## Требования и условия организационного характера

Перед эксплуатацией Системы необходимо внимательно ознакомиться с комплектом эксплуатационной документации, указанным в программном документе «Система контроля прав доступа «Матрица доступа». Спецификация» 58.29.29-001-29233469-2020, а также необходимыми организационными мерами, рекомендуемыми производителем в эксплуатационной документации.

При эксплуатации Системы должно быть обеспечено выполнение следующих условий:

* регламентация запрета использования Системы для обработки информации, содержащей сведения, составляющие государственную тайну;
* использование изделия в информационных системах 1 класса защищенности разрешается при реализации оператором требований по усилению мер защиты информации согласно методическому документу «Меры защиты информации в государственных информационных системах» (утверждены ФСТЭК России 11.02.2014);
* требования, описанные в пункте АНЗ.5 приказа ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» контроль правил генерации и смены паролей пользователей должны закрываться дополнительным ПО;
* защита информации при её передаче по каналам связи, имеющим выход за пределы контролируемой зоны, путем блокирования несанкционированного физического доступа (подключения) к ним или применения в соответствии с законодательством Российской Федерации средств криптографической защиты информации;
* при организации доступа в информационно-телекоммуникационные сети международного информационного обмена необходимо использовать сертифицированный межсетевой экран;
* использование сертифицированных ФСТЭК России версий ОС и СУБД с установленными на них актуальными обновлениями;
* наличие администратора, обеспечивающего правильную эксплуатацию изделия, в том числе:
  + предотвращение несанкционированного доступа к идентификаторам и паролям привилегированных пользователей (администратора безопасности);
  + обеспечение физической сохранности оборудования, на которое установлено изделие, и исключение возможности доступа к ним посторонних лиц
* необходимо проводить контроль целостности Системы по мере необходимости, но не реже одного раза в квартал;
* проведение процедуры создания резервных копий конфигурации изделия в соответствии с требованиями процедуры восстановления, в установленное время;
* ежедневная проверка программной среды ПЭВМ, использующейся в качестве административной консоли, на наличие вредоносного ПО;
* ежемесячный поиск актуальных уязвимостей и сведений об уязвимостях изделия и среды функционирования, анализ идентифицированных уязвимостей на предмет возможности их использования для нарушения безопасности.

## Требования и условия технического характера

Для работы Системы каких-либо особых требований и условий технического характера не предъявляется.

## Требования и условия технологического характера

Для работы Системы каких-либо особых требований и условий технологического характера не предъявляется.

# Описание задачи

* 1. Определение задачи

Система является программным средством контроля (анализа) защищенности информации, реализующим меру защиты информации «Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе» (АНЗ.5), в части:

* контроль заведения и удаления учетных записей пользователей,
* контроль реализации правил разграничения доступом,
* контроль реализации полномочий пользователей.
  1. Метод решения задачи
     1. Контроль заведения и удаления учетных записей пользователей

Система выполняет контроль заведения и удаления учетных записей пользователей в защищаемой системе – службе каталогов MS Active Directory. Контроль обеспечивается путем построения матрицы вхождения пользователей в группы безопасности службы каталогов MS Active Directory, контекстного поиска записей в сформированной матрице по пользователям и группам безопасности службы каталогов MS Active Directory, сохранения сформированной матрицы в качестве эталона и ее сравнения со сформированной матрицей текущих прав доступа пользователей защищаемой системы.

* + 1. Контроль реализации правил разграничения доступом

Система обеспечивает контроль реализации правил разграничения доступом в защищаемой системе с дискреционной либо ролевой моделями управления доступом путем построения матрицы текущих прав доступа пользователей в защищаемой системе с дискреционной, либо ролевой моделями управления доступом.

* + 1. Контроль реализации полномочий пользователей

Система выполняет контроль реализации полномочий пользователей в защищаемой системе. Контроль обеспечивается путем контекстного поиска записей в сформированной матрице доступа по объектам доступа защищаемой системы, отображения текущих прав доступа для заданного пользователя защищаемой системы с дискреционной либо ролевой моделями управления доступом; возможности сохранения сформированной матрицы текущих прав доступа пользователей в качестве эталона и ее сравнения со сформированной матрицей текущих прав доступа пользователей защищаемой системы, отображения выявленных изменений и ведения истории прав доступа.

# Входные и выходные данные

Входными данными Системы являются:

1. данные о субъектах информационных систем;
2. данные о структуре объектов доступа;
3. данные о правах доступа пользователей информационных систем;
4. данные для настроек подключения к информационным ресурсам.

Данные о субъектах информационных систем принимаются в следующем виде:

* идентификатор субъекта (SID, UID);
* связи субъектов доступа друг с другом (вхождения в группы);
* дополнительная информация о субъекте (номер телефона, электронная почта и т.д.).

Данные о структуре объектов доступа принимаются в следующем виде перечня объектов доступа с иерархией.

Данные о правах доступа пользователей информационных систем принимаются в следующем виде:

* идентификаторы субъектов;
* структура объектов доступа;
* права доступа субъектов на объекты доступа.

Данные настроек подключения к информационным ресурсам принимаются в следующем виде:

* адрес информационного ресурса;
* название информационного ресурса;
* логин пользователя для подключения к информационному ресурсу;
* пароль доступа.

Выходными данными Системы являются матрицы прав доступа информационных систем, а так же матрицы вхождения пользователей в группы, хранящиеся в БД и представляющиеся в веб-интерфейсе.

Перечень терминов

В данном документе используются следующие термины и их определения:

1. **Администратор –** лицо, ответственное за функционирование Системы контроля прав доступа «Матрица доступа» в установленном штатном режиме работы.
2. **База данных** – представленная в объективной форме совокупность самостоятельных материалов, систематизированных таким образом, чтобы эти материалы могли быть найдены и обработаны с помощью электронной вычислительной машины.
3. **Контролер** – лицо, ответственное за контроль над выполнением функций безопасности Системы контроля прав доступа «Матрица доступа».
4. **Оператор –** лицо, имеющее ограниченные привилегии по контролю выполнения функций безопасности Системы контроля прав доступа «Матрица доступа».
5. **Система доступа** – таблица, отображающая правила разграничения доступа..

# Перечень сокращений

|  |  |
| --- | --- |
| Сокращение | Полное наименование |
| **API** | Application programming interface, программный интерфейс приложения |
| **АНЗ** | Контроль (анализ) защищенности информации |
| **АРМ** | Автоматизированное рабочее место |
| БД | База данных |
| ОС | Операционная система |
| **ПО** | Программное обеспечение |
| Система | Система контроля прав доступа «Матрица доступа» |
| СУБД | Система управления базами данных |
| **ФСТЭК России** | Федеральная служба по техническому и экспортному контролю |
| ЭВМ | Электронная вычислительная машина |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Лист регистрации изменений** | | | | | | | | | |
| Изм. | Номера листов (страниц) | | | | Всего  листов  (страниц)  в докум. | № док. | Входящий № сопроводитель ного докум. и дата | Под. | Дата |
| изменен- ных | заменен-ных | новых | аннулиро-ванных |
|  |  |  |  |  |  |  |  |  |  |