ОПИСАНИЕ ФУНКЦИОНАЛЬНЫХ ВОЗМОЖНОСТЕЙ СИСТЕМЫ «ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ «ЮНИГЕЙТ»

Листов 21

Москва
2023

Аннотация

В настоящем документе представлено описание функциональных возможностей системы «Программное обеспечение «Юнигейт».

Содержание

Перечень терминов, сокращений и обозначений

В тексте настоящего документа используются термины, сокращения и обозначения, приведенные в таблице ниже (Таблица 1).

Таблица 1 – Перечень терминов, сокращений и обозначений

Термин, сокращение, обозначение	**Описание, определение, расшифровка**
Защищаемая система	Система, информационную безопасность которой обеспечивает система «Программное обеспечение «Юнигейт»
Система	Система «Программное обеспечение «Юнигейт»
СПО	Специальное программное обеспечение

1 Назначение и область применения Системы

Система «Программное обеспечение «Юнигейт» предназначена для управления учетными записями пользователей защищаемой системы, управления ролевой моделью, управления доступом пользователей к функциям и данным защищаемой системы.

Область применения – в аттестуемом по требованиям безопасности информации контуре защищаемой системы.

2 Задачи, решаемые Системой

Основными задачами, которые решает Система, являются управление учетными записями пользователей и обеспечение их безопасности, защита персональных данных и иной охраняемой законом информации, циркулирующей в защищаемой системе, в том числе:

- автоматизация управления жизненным циклом учетных записей в различных автоматизированных системах;
- обеспечение исполнения процессов и регламентов по управлению правами доступа пользователей к информационным ресурсам;
- предоставление интерфейса для работы системных администраторов и администраторов безопасности защищаемой системы;
- обеспечение возможности применять политики, регламентирующие управление доступом на основе ролей, разделение обязанностей, а также различные политики для обеспечения соответствия нормативным требованиям и рекомендациям.

3 Функциональные возможности Системы

Система «Программное обеспечение «Юнигейт» обеспечивает следующие функциональные возможности:

- авторизация и аутентификация пользователей в Системе;
- управление учетными записями пользователей;
- управление доступом пользователей к функциям и данным в защищаемой системе;
- управление ролевой моделью разграничения доступа к защищаемой системе;
- реагирование на попытки несанкционированных действий с информацией;
- протоколирование поведения пользователей в защищаемой системе;
- ведение правил проксирования;
- оповещение при наличии у одного пользователя нескольких аккаунтов для входа в защищаемую систему;
- обеспечение контроля доступа и настройки парольной политики.

3.1 Авторизация и аутентификация пользователей в Системе

Процесс авторизации и аутентификации пользователей в системе «Программное обеспечение «Юнигейт» осуществляется с использованием двухфакторной авторизации:

- первым фактором являются имя пользователя (логин) и пароль;
- вторым фактором является одноразовый код, отправляемый на электронную почту.

3.2 Управление учетными записями пользователей

Путем создания разделов «Пользователи» и «Системные пользователи» реализован единый интерфейс управления учетными записями пользователей с разделением прав на выполнение операций для:

- пользователей;
- системных администраторов;
- администраторов безопасности защищаемой системы.

Реализованы следующие возможности разделов «Пользователи» и «Системные пользователи»:

- просмотр учетных записей пользователей и их атрибутов;
- создание и редактирование учетных записей пользователей, включая форматно-логический контроль вводимых данных;
- аннулирование учетных записей пользователей;
- удаление учетных записей пользователей;
- поиск, фильтрация и сортировка учетных записей пользователей;
- выгрузка списка учетных записей пользователей;
- загрузка учетных записей пользователей;
- блокировка и снятие блокировки учетных записей пользователей;
- сброс привилегий для учетных записей пользователей;
- передача временных прав учетных записей пользователей.

Для системных администраторов реализованы следующие права в рамках реализации своих полномочий в разделах «Пользователи» и «Системные пользователи»:

- просмотр учетных записей пользователей и их атрибутов;
- создание и редактирование учетных записей пользователей и привилегированных пользователей защищаемой системы, включая форматно-логический контроль вводимых данных;
- аннулирование учетных записей пользователей;
- поиск, фильтрация и сортировка учетных записей пользователей;

- выгрузка списка учетных записей пользователей;
- загрузка учетных записей пользователей;
- блокировка учетных записей пользователей;
- сброс привилегий для учетных записей пользователей.

Для администраторов безопасности защищаемой системы реализованы следующие права в рамках реализации своих полномочий в разделах «Пользователи» и «Системные пользователи»:

- просмотр учетных записей пользователей и их атрибутов;
- создание и редактирование учетных записей системных администраторов и администраторов безопасности защищаемой системы, включая форматно-логический контроль вводимых данных;
- аннулирование учетных записей пользователей;
- удаление учетных записей пользователей;
- поиск, фильтрация и сортировка учетных записей пользователей;
- выгрузка списка учетных записей пользователей;
- блокировка и снятие блокировки учетных записей пользователей;
- сброс привилегий для учетных записей пользователей;
- передача временных прав учетных записей системных администраторов и администраторов безопасности защищаемой системы.

3.3 Управление доступом пользователей к функциям и данным в защищаемой системе

Для управления доступом пользователей к функциям и данным в защищаемой системе реализован раздел «Объекты безопасности» с возможностью ввода и вывода информации пользователю. Обеспечены следующие возможности:

- отображение объектов безопасности в виде таблицы и атрибутов объектов безопасности, в том числе:
  - статуса:
    - активен;
    - аннулирован;
  - кода;
  - наименования;
  - типа;
- отображение объектов безопасности в виде иерархического списка;
- настройка состава и расположения столбцов таблицы с объектами безопасности;
- создание объекта безопасности, в том числе на основе уже существующего;
- редактирование объекта безопасности;
- аннулирование и восстановление объектов безопасности;
- удаление объектов безопасности;
- поиск, фильтрация и сортировка объектов безопасности с помощью элементов управления на соответствующей панели.

Объекты безопасности в разделе «Объекты безопасности» отображаются в виде:

- таблицы – для линейного представления объектов безопасности;
- иерархического списка – для иерархического представления объектов безопасности.

Для настройки отображения столбцов таблицы с объектами безопасности реализована кнопка «Настройка таблицы».

Обеспечена возможность создания объекта безопасности с помощью кнопки «Добавить», в результате чего открывается форма создания объекта безопасности.

Для создания нового объекта безопасности на основе уже существующего реализована возможность выбрать только один объект безопасности в разделе «Объекты безопасности» и нажать на кнопку «Добавить на основе существующего», в результате чего открывается форма создания объекта безопасности с заполненными полями на основе значений выбранного объекта безопасности, которые доступны для изменения. При нажатии кнопки «Сохранить» выполнятся проверка на уникальность значений в полях «Код» и «Наименование».

Обеспечена возможность редактирования объекта безопасности. Для этого в разделе «Объекты безопасности» предусмотрена возможность выбрать определенный объект безопасности и нажать на кнопку «Редактировать», в результате чего открывается форма редактирования объекта безопасности с заполненными полями, которые доступны для изменения, кроме поля «Код».

Обеспечена возможность аннулирования объектов безопасности, реализованная путем логического удаления записей и присвоения им статуса «Аннулирован». Записи со статусом «Аннулирован» отображаются красным цветом и доступны только для пользователей, обладающих привилегией просмотра аннулированных записей.

Если объект безопасности имеет статус «Аннулирован», его нельзя редактировать и использовать для создания привилегий.

Обеспечена возможность восстановления объектов безопасности путем присвоения им статуса «Активен».

Для аннулирования и восстановления объектов безопасности существует возможность множественного выбора записей в разделе «Объекты безопасности». Если выбран родительский (имеющий дочерние объекты)

объект, то будут аннулированы или восстановлены все его дочерние объекты безопасности.

Удаление объектов безопасности реализовано с помощью кнопки «Удалить» в разделе «Объекты безопасности». Кнопка активна только при выборе аннулированных объектов безопасности.

Для удаления объектов безопасности реализована возможность множественного выбора объектов. Если выбран родительский (имеющий дочерние объекты) объект, то будут удалены все его дочерние объекты безопасности.

Обеспечена возможность поиска и фильтрации объектов безопасности по заданному сочетанию символов (шаблону) или выбранным значениям фильтров. Поиск и фильтрация осуществляются путем символьного сравнения введенной в поисковую строку комбинации символов, которая может находиться в любой части слова, а также выбора значения из раскрывающегося списка.

Обеспечена возможность сортировки объектов безопасности в разделе «Объекты безопасности» для упорядочивания списка объектов безопасности по выбранным пользователем параметрам. Сортировка производится по каждому столбцу таблицы с объектами безопасности при нажатии на кнопку рядом с заголовком столбца. Сортировка осуществляется в следующих режимах:

- по возрастанию – элементы упорядочиваются от меньшего к большему сверху вниз;
- по убыванию – элементы упорядочиваются от большего к меньшему сверху вниз;
- по умолчанию – включается автоматически, если выбрана сортировка по убыванию/возрастанию в другом столбце.

3.4 Управление ролевой моделью разграничения доступа защищаемой системы

Для управления ролевой моделью разграничения доступа защищаемой системы реализован раздел «Роли пользователей» с возможностью ввода и вывода информации пользователю. Обеспечены следующие возможности:

- отображение ролей пользователей и их атрибутов в виде таблицы, в том числе:
  - статуса:
    - активен;
    - аннулирован;
  - кода;
  - наименования;
  - типа роли;
  - описания;
- настройка состава и расположения столбцов таблицы с ролями пользователей;
- создание роли пользователя, в том числе на основе существующей;
- редактирование роли пользователя;
- настройка доступа пользователей к функциональности защищаемой системы;
- аннулирование и восстановление ролей пользователей;
- удаление роли пользователя;
- передача прав;
- экспорт списка ролей пользователей в файл формата PDF или XLSX;
- поиск, фильтрация и сортировка ролей пользователей с помощью элементов управления на соответствующей панели.

Роли пользователей в разделе «Роли пользователей» отображаются в виде таблицы.

Для настройки отображения столбцов таблицы с ролями пользователей реализована кнопка «Настройка таблицы».

Обеспечена возможность создания роли пользователя с помощью кнопки «Добавить» в разделе «Роли пользователей», в результате чего отображается форма создания роли с пустыми полями, которые заполняются вручную. Для создания роли реализована возможность задания атрибутов роли.

Для создания новой роли пользователя на основе уже существующей реализована возможность выбрать только одну роль пользователя в разделе «Роли пользователей» и нажать на кнопку «Создать на основе существующего», в результате чего отображается форма с заполненными полями на основе значений выбранной роли пользователя, которые доступны для изменения.

Обеспечена возможность редактирования роли пользователя. Для этого в разделе «Роли пользователей» обеспечена возможность выбрать определенную роль пользователя и нажать на кнопку «Редактировать», в результате чего отображается форма редактирования роли с заполненными полями, которые доступны для изменения.

Настройка доступа пользователей к функциональности защищаемой системы состоит в назначении для ролей пользователей набора разрешений на действия пользователей с объектами безопасности.

Процесс назначения для ролей пользователей набора разрешений на действия пользователей с объектами безопасности выполняется на вкладке «Настройка роли» (вкладка «Объекты безопасности») следующим образом: в области «Иерархия объектов безопасности» реализована возможность выбрать запись с объектом безопасности путем установки флага, в области «Привилегии» возможно выбрать требуемые привилегии путем установки флага в ячейках первого столбца таблицы (установка флага в заголовке столбца позволяет выбрать все записи на странице). Сохранение изменений

происходит после нажатия кнопки «Сохранить», отмена изменений происходит путем нажатия кнопки «Отмена».

Обеспечена возможность аннулирования и восстановления ролей пользователей. Если роль пользователя имеет статус «Аннулирован», ее нельзя редактировать и использовать для назначения пользователю. Для пользователей с уже назначенной ролью, которая аннулируется, снимаются привилегии, связанные с данной ролью.

Для аннулирования и восстановления ролей пользователей реализована возможность множественного выбора записей в разделе «Роли пользователей».

Обеспечена возможность передачи прав учетных записей пользователей. Считывание прав учетной записи пользователя осуществляется для конкретной выбранной учетной записи пользователя в разделе «Пользователи» по нажатию кнопки «Передать права».

Обеспечена возможность выгрузки ролей пользователей. При нажатии кнопки «Экспорт» раскрывается список, состоящий из элементов «Экспорт в формате XLSX» и «Экспорт в формате PDF».

Обеспечена возможность поиска и фильтрации ролей пользователей по заданному сочетанию символов и заданным значениям фильтров. Поиск и фильтрация осуществляются путем символьного сравнения введенной в поисковую строку комбинации символов, которая находится в любой части слова, а также выбора значения из раскрывающегося списка.

Поиск ролей пользователей осуществляется без учета регистра по любому вхождению по значению полей «Код» и «Наименование».

Фильтрация ролей пользователей осуществляется с помощью фильтров «Код», «Наименование», «Тип роли», «Объект безопасности» и «Статус».

Обеспечена возможность сортировки ролей пользователей в разделе «Роли пользователей» для упорядочивания списка ролей пользователей по выбранным пользователем параметрам. Сортировка производится по каждому

столбцу таблицы с ролями пользователей при нажатии на кнопку рядом с заголовком столбца. Сортировка осуществляется в следующих режимах:

- по возрастанию – элементы упорядочиваются от меньшего к большему сверху вниз;
- по убыванию – элементы упорядочиваются от большего к меньшему сверху вниз;
- по умолчанию – включается автоматически, если выбрана сортировка по убыванию/возрастанию в другом столбце.

3.5 Реагирование на попытки несанкционированных действий с информацией

В рамках реагирования на попытки несанкционированных действий с информацией администратор безопасности защищаемой системы, обладающий специальными правами, производит настройки функций (включить/выключить и настроить параметры), используемых для решения соответствующих задач, в том числе:

- установить необходимость прохождения двухфакторной авторизации;
- установить запрет на использование идентификаторов удаленных пользователей в течение заданного времени (в календарных днях);
- установить число неудачных попыток ввода пароля в течение заданного периода времени, после которых блокируется учетная запись пользователя на заданный промежуток времени;
- установить период времени, по истечении которого происходит сброс счетчика неудачных попыток входа.

Факты неуспешных попыток входа в защищаемую систему и блокировки пользователей фиксируются в разделе «Протокол». В табличном представлении раздела «Протокол» действия, которые не санкционированы политикой безопасности, выделены красным цветом.

Администратор безопасности защищаемой системы имеет возможность снять блокировку учетной записи пользователя при просмотре перечня учетных записей пользователей в разделах «Пользователи», «Системные пользователи» или при просмотре учетной записи конкретного пользователя.

На вкладке «Настройки безопасности» (вкладка «Контроль доступа») раздела «Настройка» реализована возможность установить необходимость прохождения двухфакторной авторизации, при этом:

- при установленном флаге «Двухфакторная авторизация» задействована двухфакторная авторизация (логин/пароль и проверка с помощью одноразового кода) пользователя для доступа в защищаемую систему;
- при снятом флаге «Двухфакторная авторизация» не задействована двухфакторная авторизация, для доступа пользователя в защищаемую систему используются только логин и пароль.

На вкладке «Настройки безопасности» (вкладка «Контроль доступа») раздела «Настройка» реализована возможность установить запрет на использование идентификаторов удаленных пользователей в течение заданного времени (в календарных днях), при этом:

- при установленном флаге «Запретить повторное использование идентификаторов удаленных пользователей (в днях)» обеспечивается сохранение логина удаленной учетной записи пользователя в отдельный реестр и хранение его в течение N дней, где параметр N – целое число от 1 до 1827 (5 лет);
- при снятом флаге «Запретить повторное использование идентификаторов удаленных пользователей (в днях)» функция отключена.

При достижении максимального количества неудачных попыток ввода пароля осуществляется блокировка учетной записи пользователя и отображается сообщение о блокировке.

На вкладке «Настройки безопасности» (вкладка «Парольная политика») раздела «Настройка» настроен сброс счетчика неудачных попыток входа через указанное число минут.

3.1 Присвоение ролей и привилегий группам пользователей в защищаемой системе

Для присвоения ролей и привилегий группам пользователей в защищаемой системе реализован раздел «Группы пользователей», обеспечивающий следующие возможности:

- отображение групп пользователей и их атрибутов в виде таблицы, в том числе:
  - кода;
  - наименования;
- настройка состава и расположения столбцов таблицы с группами пользователей;
- редактирование группы пользователей;
- настройка группы пользователей с учетом функциональности защищаемой системы;
- удаление группы пользователей;
- поиск, фильтрация и сортировка групп пользователей с помощью элементов управления на соответствующей панели.

3.2 Протоколирование поведения пользователей в защищаемой системе

Для осуществления протоколирования поведения пользователей в защищаемой системе реализованы функции протоколирования событий безопасности, мониторинга сессий пользователя в виде разделов «Протокол» и «Мониторинг сессий».

Раздел «Протокол» обеспечивает:

- отображение событий безопасности в виде таблицы;

- настройку отображения таблицы: набора столбцов, их расположения;
- сортировку событий безопасности;
- поиск и фильтрацию протоколируемых событий;
- выделение в табличном представлении протоколируемых действий пользователей тех действий, которые запрещены политикой безопасности;
- экспорт протокола событий в файл формата PDF;
- создание и просмотр резервных копий протокола событий.

Раздел «Мониторинг сессий» обеспечивает:

- отображение активных сессий СПО защищаемой системы в табличном виде;
- настройку отображения таблицы: набора столбцов, их расположения;
- сортировку активных сессий;
- поиск и фильтрацию сессий СПО защищаемой системы;
- прекращение выбранных активных сессий;
- обновление списка активных сессий;
- экспорт списка активных сессий в файл формата PDF.

3.3 Ведение правил проксирования

Для ведения правил проксирования реализованы следующие функциональные возможности раздела «Правила проксирования»:

- отображение правил проксирования и их атрибутов;
- создание и редактирование правил проксирования;
- удаление правил проксирования;
- поиск, фильтрация и сортировка правил проксирования.

3.4 Оповещение при наличии у одного пользователя нескольких аккаунтов для входа в защищаемую систему

Для оповещения при наличии у одного пользователя нескольких аккаунтов для входа в защищаемую систему обеспечены следующие возможности:

- настройка максимального числа активных сессий;
- контроль максимального числа активных сессий:
  - при установленном флаге ограничивается количество параллельных активных сессий пользователя в защищаемой системе в количестве N штук, где параметр N – целое число от 1 до 9;
  - при снятом флаге разрешена только одна активная сессия при работе пользователя с защищаемой системой.

Настройка максимального числа активных сессий выполняется:

- в разделе «Пользователи»: личные ограничения максимального числа активных сессий;
- в разделе «Роли пользователей»: ролевые ограничения максимального числа активных сессий;
- в разделе «Настройка»: общесистемные ограничения максимального числа активных сессий.

3.5 Обеспечение контроля доступа и настройки парольной политики

Для обеспечения реагирования на попытки несанкционированных действий с информацией реализована возможность контроля доступа, а также возможность настройки парольной политики. Для обеспечения данных функциональных возможностей в разделе «Настройка» реализованы вкладки «Контроль доступа» и «Парольная политика».

Вкладка «Контроль доступа» позволяет администратору безопасности защищаемой системы, обладающему специальными правами, произвести

настройки функций (включить/выключить и настроить параметры, настроенная конфигурация сохраняется), используемых для решения задач контроля доступа.

Вкладка «Парольная политика» позволяет администратору безопасности защищаемой системы, обладающему специальными правами, производить настройки функций (включить/выключить и настроить параметры, настроенная конфигурация сохраняется), используемых для решения задач настройки парольной политики.