«Инфомаксимум»
(Общество с ограниченной
ответственностью)

Proceset

Руководство администратора информационной безопасности

2019 г.

Содержание

1. Общие положения

1.1 Основные термины

Термин	Описание
GraphQL	стандарт декларирования структуры данных и способов получения данных, который выступает дополнительным слоем между клиентом и сервером
Https	расширение протокола HTTP для поддержки шифрования в целях повышения безопасности. Данные в протоколе HTTPS передаются поверх криптографических протоколов SSL или TLS
PBKDF2	функция получения ключа, разработанная RSA Laboratories, используемая для получения стойких ключей на основе хэша
RocksDB	высокопроизводительная встраиваемая СУБД на основе LSM-tree с открытым исходным кодом (лицензия Apache 2.0) от компании Facebook
SHA256	представляет собой однонаправленную функцию для создания цифровых отпечатков фиксированной длины (256 бит, 32 байт) из входных данных размером до 2,31 эксабайт (2^{64} бит) и является частным случаем алгоритма из семейства криптографических алгоритмов SHA-2 (Secure Hash Algorithm Version 2) опубликованным АНБ США в 2002 году
Агент мониторинга	приложение proceset.agent, которое устанавливается на компьютер сотрудника и собирает статистику об его активности
Активность сотрудника	сведения о работе сотрудника за компьютером
Карта процесса	схема последовательности событий (операций, которые осуществляют сотрудники в ходе выполнения процесса), и связей между ними
Профиль сотрудника	информация о сотруднике компании, включающая общие сведения, настройки доступа и список источников сбора информации
Репозиторий	место, где хранится и поддерживается исходный код системы
Соль	строка данных, которая передаётся хеш-функции вместе с паролем
Хеш пароля	преобразованный массив входных данных (пароля) произвольной длины в (выходную) битовую строку установленной длины, выполняемое определённым алгоритмом (SHA256)

1.3 Основные сокращения

Сокращение	Описание
АБ	Администратор информационной безопасности
АС	Автоматизированная система
ЖА	Журнал аудита
ИБ	Информационная безопасность
ИС	Информационная система
ОС	Операционная система
РД	Роль доступа

2. Общее описание

2.1 Назначение документа

Данное Руководство является основой для реализации практических мер по обеспечению информационной безопасности (далее – ИБ) при эксплуатации. автоматизированной системы «Система управления рабочим временем» на базе решения Proceset/CrocoTime (далее - Система).

В документе содержится информация о средствах, реализующих безопасность и сохранность целостности данных на уровне операционной системы и прикладного программного обеспечения, приводятся необходимые сведения по использованию данных средств с целью защиты от несанкционированного доступа к информации Системы, а также для предотвращения несанкционированных вмешательств в работу Системы.

Документ предназначен для персонала, основной обязанностью которого является обеспечение информационной безопасности.

2.2 Функции администратора безопасности

Администратор информационной безопасности (далее АБ) осуществляет:

- Просмотр списка пользователей Системы, в том числе активных;
- Просмотр и контроль прав доступа пользователей Системы;
- Выявление событий несанкционированного доступа к Системе или данным, обрабатывающимся в Системе с использованием ЖА Системы;
- Направление требований по блокированию пользователей Системы при выявлении событий несанкционированного доступа (попыток совершения несанкционированного доступа) к Системе или данным, обрабатывающимся в Системе, Прикладному администратору Системы.

3. Описание механизма аудита

3.1 Выявление неправомерных действий

Для выявления неправомерных действий в Системе необходимо использовать инструмент логирования событий. Журнал событий безопасности по умолчанию располагается: C:\Program Data\Infomaximum\logs\security.log. Более подробная информация указана в п.9

Для выявления неправомерных действий необходимо использовать журнал аудита (см. п. 9), а также воспользоваться описанием процесса выявления неправомерных действий (Таблица 1).

Таблица 1

Описание процесса выявления неправомерных действий

Неправомерное действие	Описание
Входы в систему с разными ID пользователя с одной рабочей станции в короткие интервалы времени (интервал устанавливается экспертами)	Вход 1 (действие 1) - Тип события: logon - Доп. параметр типа события: success - Объект: id - Адрес рабочей станции: remote_address - Поле: Время события Вход 2 (действие 2) - Тип события: logon - Доп. параметр типа события: success - Объект: id - Адрес рабочей станции: remote_address

Неправомерное действие	Описание
	- Поле: Время события Если параметры ID объекта отличаются, а remote_address имеют одинаковое значение, то Время события 1 – Время события 2 = интервал входа с одной рабочей станции (интервал сравнивается с установленным параметром)
Вход с одним и тем же ID пользователя с разных рабочих станций в короткие интервалы времени (интервал устанавливается экспертами)	Вход 1 (действие 1) - Тип события: logon - Доп. Параметр типа события: success - Объект: id - Адрес рабочей станции: remote_address - Поле: Время события Вход 2 (действие 2) - Тип события: logon - Доп. параметр типа события: success - Объект: id - Адрес рабочей станции: remote_address - Поле: Время события Если ID имеют одинаковое значение, а значения remote_address отличаются, то Время события 1 – Время события 2 = интервал входа с одной рабочей станции (интервал сравнивается с установленным параметром)
Большое количество неудачных входов в систему с одним ID с разных терминалов	- Тип события: logon - Доп. параметр типа события: invalid_logon - Объект**:** id - Адрес рабочей станции: remote_address Или - Тип события: logon - Доп. Параметр типа события: max_logon_attempts_exceed - Объект**:** id - Адрес рабочей станции: remote_address, где remote_address имеют разные значения в каждой попытке входа.
Большое количество неудачных входов в систему с разными ID с одного терминала	- Тип события: logon - Доп. параметр типа события: invalid_logon - Объект**:** id - Адрес рабочей станции: remote_address Или - Тип события: logon - Доп. параметр типа события: max_logon_attempts_exceed - Объект**:** id - Адрес рабочей станции: remote_address, где remote_address имеют одинаковое значение в каждой попытке входа.
Попытка входа в систему с заблокированной учётной записью	- Тип события: logon - Доп. Параметр типа события: disabled_logon - Объект**:** id
Отключение логирования	Для конфигурирования логов используется файл конфигурации: C:\ProgramData\Infomaximum\logback.xml, также есть вариант с подменой конфигурации посредством механизма инициализации системы логирования. Подробный порядок и загрузки файла конфигурации описан: https://logback.qos.ch/manual/configuration.html Рекомендации: Необходимо отслеживать изменение в каталоге: C:\ProgramData\Infomaximum Необходимо отслеживать изменение в каталоге: C:\Program Files\Infomaximum

Неправомерное действие	Описание
	Необходимо отслеживать изменения службы.
Удаление / очистка логов	Удаление и очистка логов не может осуществляться через веб-интерфейс, логирование данного неправомерного действия не осуществляется. Доступ к удалению/очистке логов регламентируется на уровне файловой системы в рамках windows-политик.
Добавление нового ID пользователя в систему и его удаление (блокировка) в короткий промежуток времени (короткий промежуток времени устанавливается экспертами)	Субъект (тот, кто производит действие): - Объект**:** id - Адрес рабочей станции: remote_address - Сотрудник: employee_id - Действие 1(тип события): create (создание) - Действие 2 (тип события): remove (удаление) - Действие 3 (тип события): change_enabled_logon - Доп. параметр действия 3: - false (отключение разрешения на авторизацию, блокировка) - Поле: Время события (для каждого действия) Объект (над кем производят действие): - Объект**:** id - Объект: employee Если ID объекта (добавляемого сотрудника) имеет одинаковое значение при всех действиях, то Время события действия remove – Время события действия create = интервал времени между созданием и удалением сотрудника; или Время события действия change_enabled_logon (доп. параметр: - false) – Время события действия create = интервал времени между созданием и блокировкой сотрудника;
Назначение новых прав / членства в группе пользователю и их последующая отмена в короткий интервал времени *(*интервал устанавливается экспертами*)*	Субъект (тот, кто производит действие): - Объект**:** id - Адрес рабочей станции: remote_address - Сотрудник: employee_id - Действие 1 (Тип объекта): adding_access_role_id (Добавление сотруднику РД) - Действие 2 (Тип объекта): removing_access_role_id (удаление у сотрудника РД в группе «Административные» роли) Доп параметр у всех типов объектов (всех действий): access_role_id (id роли доступа) access_role_name (имя роли доступа) - Поле: Время события (для каждого действия) Объект (над кем производят действие): - Объект**:** id, employee, login Если ID и Login объекта (над кем производят действие) имеет одинаковое значение при всех действиях, и назначаемая и отменяемая РД имеет одинаковое значение access_role_id, то Время события действия removing_access_role_id – Время события действия adding_access_role_id = интервал времени между назначением новых прав и их последующая отмена.
Изменение парольной политики АС	- Объект**:** id - Адрес рабочей станции: remote_address - Сотрудник: employee_id, login - Действие 1 (Тип объекта): change_complex_password_setting (Включение/выключение проверки безопасности пароля) - Действие 2 (Тип объекта): change_min_password_length_setting (Изменение минимальной длины пароля)

Неправомерное действие	Описание
	- Действие 3 (Тип объекта): change_password_expiration_time_setting (Изменение времени жизни пароля) - Действие 4 (Тип объекта): change_max_invalid_logon_count_setting (Изменение лимита на неуспешные попытки входа) Любое изменение из 4 типов событий (действий) является изменением парольной политики АС;

4. Работа с базой данных

Доступ к базе данных защищается на уровне файловой системы. Для просмотра базы данных необходимо использовать специальную утилиту.

4.1 Просмотр базы данных

Для просмотра базы данных необходимо:

- Запустить утилиту для просмотра базы данных «rdao-viewer-0.1.1.exe»;
- Перейти по следующему пути: File/Open database (ReadOnly) или File/Open database;
- Выбрать необходимую папку с базой данных. По умолчанию папка с базой данных Системы находится: C:\ProgramData\Infomaximum\database.

4.2 Структура хранения паролей

Для просмотра структуры хранения паролей пользователей необходимо использовать инструмент rdao-viewer-0.1.1.exe.

Для просмотра структуры хранения паролей пользователей необходимо:

- Запустить утилиту для просмотра базы данных «rdao-viewer»;
- Перейти по следующему пути: File/Open database (ReadOnly) или File/Open database;
- Выбрать необходимую папку с базой данных. По умолчанию папка с базой данных Proceset находится по пути: C:/ProgramData/Infomaximum/database;
- Выбрать строку (columnFamily): com.infomaximum.subsystem.core.Employee;
- В столбце «Key» указаны ключи записей базы данных, а в поле «Value» значение каждого ключа;
- Значение ключа «password_hash» (пароль пользователя) записано в хешированом виде.

4.3 Резервное копирование

Система периодически (раз в сутки, в 00:00:00) выполняет резервное копирование (бэкап базы данных). Резервное копирование по умолчанию осуществляется в системную папку: C:/ProgramData/Infomaximum/backup.

Параметры базы данных настраиваются в файле: com.infomaximum.subsystem.database.json.

Путь к файлу: C:/ProgramData/Infomaximum/config/com.infomaximum.subsystem.database.json.

Контроль целостности по контрольным суммам осуществляется при каждой загрузке Системы. Периодически в процессе работы Системы контроль целостности по контрольным суммам не осуществляется. В состав Системы встроены средства отладки, которые невозможно удалить, но можно контролировать его активацию, для этого необходимо отслеживать все изменения в службе «infomaximum», в частности, команду запуска. Восстановить БД возможно с помощью специальной утилиты. (см. п. 4.2)

4.4 Сохранение копии обезличенной базы данных

Для сохранения обезличенной БД Системы необходимо чтобы у пользователя Системы была назначена роль доступа с включенной привилегией «Общие настройка системы» с операцией доступа W (изменение).

Сохранение обезличенной БД можно произвести двумя способами:

- Через веб-интерфейс Системы на странице «Настройки» / «Настройки системы» / «База данных»

Для запуска процесса необходимо указать путь (директорию), куда сохранится обезличенная БД.

- Через GraphQL при выполнения следующего запроса:

```
mutation{
  database{
    copy_depersonalized_database(path:"c:/database")

  }
}
```

Где, «c:/database» путь сохранения обезличенной БД.

Для выполнения запроса GraphQL у пользователя должна быть назначена роль доступа с включенной привилегией «Инструмент GraphQL» с операцией доступа R.

Сохранение происходит на сервер, где установлена Система. Папка для сохранения должна быть создана заранее и должна быть пустой.

5. Мониторинг состояния системы

5.1 Правила контроля неизменности

Для контроля работоспособности системы необходимо:

- Для ручной проверки: открыть страницу – http://localhost:8010/;
- Для автоматической проверки отправить GraphQL запрос вида: {server{status}}. Инструкция по выполнению GraphQL запросов представлена в п. 6.
- Отслеживать событие журнала аудита с объектом) «system» (target@729368). Подробнее в п.9

5.2 Работоспособность системы

Для контроля неизменности системы необходимо отслеживать:

- Контрольные суммы файлов в папке: C:\Program Files\Infomaximum;
- Наличие новых файлов в папке: C:\Program Files\Infomaximum;
- Команду запуска службы: Infomaximum;
- Контрольную сумму файла: C:\ProgramData\Infomaximum\logback.xml;
- События в логе: C:\ProgramData\Infomaximum\logs\security.log.

6. Работа с GraphQL

6.1 Описание GraphQL

GraphQL – это стандарт декларирования структуры данных и способов получения данных, предложенный и описанный Facebook, который обеспечивает более эффективную и гибкую альтернативу REST.

Официальный сайт и документация: https://graphql.org/. Для более удобного формирования и выполнения запросов, в поставку включен инструмент GraphQL, для его использования необходимо:

- Авторизоваться в Системе;
- Перейти по адресу: http://localhost:8010/graphiql

С кратким описанием работы с GraphQL можно ознакомиться по следующим ссылкам:

- https://medium.com/the-graphqlhub/graphiql-graphql-s-killer-app-9896242b2125
- https://medium.com/graphql-mastery/graphql-quick-tip-how-to-pass-variables-into-a-mutation-in-graphiql-23ecff4add57

GraphQL API — поддерживает автогенерацию документации. Документация всегда находится в актуальном состоянии. Местоположение документации: http://localhost:8010/graphiql, вкладка «Docs» (которая находится в верхнем правом углу).

6.2 Пример запроса

```
1    {
2      server{
3        status
4      }
5      employee{
6        employees{
7          id
8
9    display_name
10       }
11     }
     }
```

Для выполнения запроса из внешней системы:

- Сгенерировать Ключ API: «Меню/Настройки/Настройки системы/Ключи API»
- Выполнить взаимную аутентификацию с помощью сертификатов

7. АРМ Администратора ИБ

7.1 Управление пользователями Системы

7.1.1 Просмотр списка пользователей

Существует два варианта для просмотра списка пользователей Системы:

- Через веб-интерфейс Системы. Список пользователей находится в п.е «Настройки/ «Настройки компании» / «Сотрудники»;
- С использованием GraphQL запроса:

```
{
  employee {
    employees {
      id
      email
      display_name
      enabled_logon
      access_roles {
        items {
          id
          name
        }
      }
    }
  }
}
```

7.1.2 Просмотр списка активных пользователей

Для получения списка активных пользователей Системы необходимо выполнить следующий GraphQL запрос:

```
{
  employee{
    employee_tree(enabled_logon:true) {
      elements {
        element {
          ... on employee {
            id
            display_name
            enabled_logon
          }
        }
      }
    }
  }
}
```

7.1.3 Просмотр истории изменения пользователей

Для просмотра истории изменения пользователей необходимо использовать ЖА. Событие о изменении пользователя обязательно содержит в строке следующую запись: [target@729368 id="1" type="employee"], где id – это номер сотрудника. Запись об изменении параметра сотрудника в ЖА имеет вид: [event@729368 type="change_enabled_logon" old_value="true", new_value="false"], где type – это изменяемый параметр, old_value – старое значение, new_value – новое значение.

Для просмотра всех характеристик сотрудника необходимо:

- Перейти через веб-интерфейс АС в Профиль конкретного сотрудника: Настройки /Настройки компании/Сотрудники/Профиль сотрудника;

7.1.4 Блокировка пользователей в системе

Блокирование пользователей в системе возможно через веб-интерфейс Системы. Блокирование осуществляется на вкладке: «Настройки/ «Настройки компании» / «Сотрудники». Необходимо выбрать пользователей, которым нужно ограничить доступ и через функцию «массовое назначение» перевести значение «Доступ в систему» в состояние «отключено».

```
            mutation {
              employee {
                update(id:1
                enabled_logon:false) {
                  id
                  enabled_logon
                }
              }
    }
```

7.2 Управление группами Системы

7.2.1 Просмотр списка групп

Просмотр списка групп возможен двумя способами:

- Через веб-интерфейс Системы. Список групп находится в разделе «Настройки/ «Настройки компании» / «Сотрудники».
- Отправка GraphQL-запроса следующего формата:

```
{
```

```
department{
  departments{
    id
    name
   }
  }
}
```

Основы работы с GraphQL описаны в п. 6.

7.2.2 Просмотр изменения групп

Для просмотра изменения групп необходимо использовать GraphQL запрос:

```
{
  department{
    department (id:1) {
      id
      name
    }
  }
}
```

где, `id:1` – номер конкретной группы.

Для сравнения необходимо выполнить два или более запроса, первый запрос – выполняем в начале анализируемого периода, второй запрос – в конце анализируемого периода. Отличия в ответах указывают на изменение параметров. Основы работы с GraphQL описаны в п. 6настоящего руководства

7.3 Управление ролями доступа Системы

7.3.1 Просмотр списка ролей доступа

Существует два варианта просмотра списка РД:

- Через веб-интерфейс АС. Список ролей находится в разделе «Настройки/ «Настройки компании» / «РД».
- Отправка GraphQL запрос следующего формата:

```
{
  list{
    core_list{
      access_role_list{
        items{
          element{
            __typename
            id
            name
          }
        }
      }
    }
  }
}
```

Основы работы с GraphQL описаны в п. 6 настоящего руководства.

8. Реализованные защитные меры ИБ в Системе

8.1 Аутентификация пользователей в Системе

Механизм аутентификации в Системе происходит следующим образом:
У каждого пользователя системы существует логин и пароль. Для возможности входа в систему необходимо чтобы учётная запись пользователя вместе с логином и паролем

существовала в системе. При входе происходит проверка подлинности пользователя путём сравнения хеша введённого им пароля (для указанного логина) с хешем пароля, сохранённым в базе данных. Для пароля применяются определенные требования, более подробно можно ознакомиться в п. 8.3

8.2 Перечень объектов защиты системы

Перечень защищаемых объектов:

- Журналы аудита (хранятся в логах C:\ProgramData\Infomaximum\logs);
- Аутентификационная информация пользователей (хранится в базе C:\ProgramData\Infomaximum\database);
- Файлы настроек (хранится в базе C:\ProgramData\Infomaximum\database);
- Права доступа (хранится в базе C:\ProgramData\Infomaximum\database);
- Механизмы настройки прав и аудита (хранится в базе C:\ProgramData\Infomaximum\database);
- Исполняемые файлы (расположение C:\Program Files\Infomaximum);
- Элементы интерфейса для веб (расположение C:\Program Files\Infomaximum);

Необходима защита на уровне операционной системы следующих каталогов:

- C:\Program Files\Infomaximum;
- C:\ProgramData\Infomaximum.

Для валидации сертификатов используется стандартное Windows хранилище.

8.3 Проверка безопасности пароля пользователей (Сложный пароль)

Проверка безопасности пароля пользователей включает в себя следующие ограничения на установку/изменение пароля в системе:

- прописные буквы английского алфавита от A до Z;
- строчные буквы английского алфавита от a до z;
- десятичные цифры (от 0 до 9);
- неалфавитные символы (например, !, $, #, %)
- длина пароля;
- запрет на повторное использование уже использованных паролей.

Проверка соблюдения этих требований выполняется при изменении или создании паролей. Произвести настройку параметра возможно через веб-интерфейс: «Настройки»/ «Настройки системы»/ «Безопасность». Проверка на содержания в пароле символов из e-mail отсутствует. Просмотр настройки параметров доступны также через веб-интерфейс по указанному адресу выше.

8.4 Минимальная длина пароля

Настройка минимальной длины пароля доступна только в случае, если включен параметр «Проверка безопасности пароля». Произвести настройку параметра возможно через веб-интерфейс: «Настройки»/«Настройки системы»/«Безопасность». Параметр указывает минимально допустимое количество символов при создании/изменении пароля. Допустимые значения: от 8 до 15 символов. Если параметр «Проверка безопасности пароля» находится в состоянии «Выкл.», то минимальное количество символов по умолчанию – 4. Просмотр настройки параметров доступны также через веб-интерфейс по указанному адресу выше.

8.4 Срок действия пароля

Параметр «Срок действия пароля» указывает срок действия пароля с момента его задания/изменения. Если параметр находится в состоянии «Вкл.», то возможно указать его значение. Возможное значение параметра – от 1 до 1000 дней. После того, как срок действия завершился, пользователю предлагается задать новый пароль.

Если после окончания действия пароля пользователь пытается авторизоваться в системе под своим паролем (у которого закончился срок действия), то ему предлагается задать новый пароль. Пока пользователь не задаст новый пароль, доступ в систему будет ограничен.

При состоянии «Выкл.» параметр «Срок действия пароля» становится неактивным, и в этом случае действие пароля не ограничено по времени. Произвести настройку параметра возможно через веб-интерфейс: «Настройки»/ «Настройки системы»/ «Безопасность».

Если параметр «Сложный пароль» находится в состоянии «Выкл.», то пользователь при вводе нового пароля может использовать предыдущие пароли, за исключением последнего заданного пароля.

Если срок действия пароля не истёк, но сотрудник поменял пароль на тот же (который установлен у него в данный момент), то счётчик срока действия пароля не обнуляется. Если пользователь поменял пароль на другой (хотя срок действия пароля не закончился) счётчик срока действия обнуляется и идёт отсчёт согласно заданному параметру. Произвести настройку параметра возможно через веб-интерфейс: «Настройки»/«Настройки системы»/ «Безопасность». Просмотр настройки параметров доступны также через веб-интерфейс по указанному адресу выше.

8.5 Шифрование пароля

При авторизации в Системе происходит взаимодействие между МНА (веб-интерфейс) и сервером. На сервер не отправляется введённый пользователем пароль в исходном виде. МНА отправляет на сервер Хеш пароля. Хеширование пароля происходит с помощью алгоритма SHA256.

Сервер получает хеш пароля и использует хеш функцию повторно, а также функцию, формирующую секретный ключ по стандарту PBKDF2 (PBKDF2WithHmacSHA512). Сервер сохраняет в базе 2 значения в виде секретного ключа: Соль + Хеш (от присланного хеша пароля). Просмотр настройки параметров доступны также через веб-интерфейс по указанному адресу выше.

8.6 Количество попыток входа

Возможные значения параметра «Ограничение количества попыток входа»: «Вкл.»/ «Выкл.». Если параметр включен, то ограничения по количеству попыток входа активируется, и становится активным параметр «Количество допустимых попыток входа». Если параметр выключен, то параметр «Количество допустимых попыток входа» недоступен и ограничения на количество попыток входа отсутствуют. Произвести настройку параметра возможно через веб-интерфейс: «Настройки»/ «Настройки системы»/ «Безопасность». Просмотр настройки параметров доступны также через веб-интерфейс по указанному адресу выше.

Допустимое значение параметра «Количество попыток входа» – от 1 до 100. Параметр отвечает за количество попыток входа, которые пользователь может совершить в Системе. (попытка входа – когда пользователь верно указал логин, но неправильно ввёл пароль и нажал «войти»).

Произвести настройку параметра возможно через веб-интерфейс: «Настройки»/ «Настройки системы»/«Безопасность». Если попытки достигают заданного параметра, пользователь блокируется, данному пользователю ограничивается вход в систему, Администраторам системы отправляется письмо на указанный e-mail (параметр «Электронная почта» в «Настройки»/«Настройки компании»/«Сотрудники»/«Профиль сотрудника») о

блокировке пользователя. Просмотр настройки параметров доступны также через веб-интерфейс по указанному адресу выше.

Администраторами системы являются все пользователи, у которых в группе ролей «Административные» параметр «Управление настройками системы» и параметр «Редактирование сотрудников» находится в состоянии «Вкл». Если у администратора в его профиле сотрудника («Настройки»/ «Настройки компании»/«Сотрудники»/«Профиль сотрудника») параметр «Оповещение о блокировке пользователей сотрудника» находится в состоянии «Выкл.», то письмо на почту данного Администратора отправлено не будет. Параметр «Оповещение о блокировке пользователей сотрудника» невозможно включить, если не произведены или некорректно произведены настройки почтового сервера. («Настройки»/ «Настройки системы»/ «Почтовый сервер»).

Период, после которого попытки входа пользователя обнуляются, по умолчанию составляет 10 минут. (То есть, если между попытками ввода учетных данных не более 10 минут, то они считаются последовательными как 1,2,3,4 и т.д. и по заданному значению «Количество допустимых попыток» аккаунт блокируется). Как только проходит 10 минут счётчик сбрасывается.

Изменение периода возможно посредством конфигурационного файла. Для изменения периода, после которого происходит обнуление попыток входа необходимо:

- перейти по пути: C:\ProgramData\Infomaximum\config;
- открыть файл конфигурации: infomaximum.subsystem.core.json;
- изменить значение параметра: `reset_count_invalid_logon_duration` (значение можно указать в днях, часах, минутах и секундах).

8.7 Срок жизни ссылки на восстановление пароля

В случае, если пользователь забыл пароль, он может быть восстановлен посредством почты. Письмо будет отправлено только в том случае, если произведены настройки почтового сервера в системе Proceset («Настройки»/«Настройки системы»/«Почтовый сервер»). В письме указывается ссылка, после перехода по которой пользователь может создать новый пароль согласно настройкам парольной политики. По умолчанию параметр «Срок жизни ссылки для восстановления пароля» имеет значение 1 день (24 часа). Изменение параметра через веб-интерфейс недоступно. Изменение периода возможно через конфигурационный файл.

Для изменения периода необходимо:

- открыть папку: C:\ProgramData\Infomaximum\config;
- открыть файл конфигурации: com.infomaximum.subsystem.core.json;
- изменить параметр `restorelink_timeout` (значение можно указать в днях, часах, минутах и секундах).

8.8 Время жизни неактивной сессии

По умолчанию период жизни неактивной сессии для каждого пользователя – 1 неделя (7 дней). Изменение параметра через веб-интерфейс недоступно. Изменение периода возможно через конфигурационный файл.

Для изменения периода необходимо:

- открыть папку: C:\ProgramData\Infomaximum\config;
- открыть файл конфигурации: com.infomaximum.subsystem.fronted.json;
- изменить параметр: `session_timeout` (значение можно указать в днях, часах, минутах и секундах)
- перезапустить службу «infomaximum»

8.9 Идентификация, аутентификация субъектов и объектов доступа

Для всех пользователей и программных процессов осуществляется идентификация, аутентификация и авторизация. Пользователю, не прошедшему аутентификацию, не предоставляется доступ в Систему. В Системе существуют механизмы управления учетными записями пользователей: создание, активация, блокирование, предоставление и изменение прав и т.д. В Системе применяется локальная аутентификация.

Для управления компонентами Системы требуется собственная авторизация, при этом выполняются следующие требования:

- при входе осуществляется идентификация и проверка подлинности субъектов доступа;
- пароль-хеш и идентификаторы передаются исключительно по сети и хранятся в зашифрованном виде;
- отсутствует возможность изменить пароль методом замены объекта, хранящего зашифрованный пароль;
- реализована возможность установления минимальной длины (не менее 8 символов) и срока действия пароля (парольная политика);
- реализована возможность установления уровня сложности пароля (парольная политика);
- реализована возможность установления запрета на повторное использование одного и того же пароля (парольная политика);
- пользователю предоставляется право самостоятельно изменять свой пароль;
- в системе отсутствует доступ Администраторов системы к паролю пользователя;
- в системе осуществляется контроль и подсчет попыток входа в Систему (успешный или неуспешный – несанкционированный);
- в системе предусмотрена настройка блокировки входа пользователя до разблокирования администратором системы или при достижении заданного числа неуспешных попыток входа;
- система уведомляет пользователя о превышении количества неудачных попыток входа. После превышения заданного количества неудачных попыток входа доступ не предоставляется, также при предъявлении правильного пароля, пользователь не информируется о вводе правильного пароля;
- система позволяет производить блокировку сеанса по запросу субъекта.

8.10 Блокировка пользователей Системы

Блокирование пользователей возможно осуществить следующими способами:

1. Через веб-интерфейс (Настройки компании/Сотрудники/Профиль сотрудника), перевести значение «Доступ в систему» у нужного сотрудника в состояние «Выкл» или через массовые действия (Настройки компании/Сотрудники), предварительно выбрав нужных сотрудников;

2. С использованием GraphQL запроса для блокировки из внешней АС. Для блокировки пользователя необходимо отправить запрос вида:

```
mutation{
    employee{
        update(id: 2,
enabled_logon: false) {
            id
        }
    }
}
```

Где id – идентификатор пользователя.

Инструкция по выполнению GraphQL запросов представлена в Руководстве прикладного администратора, п.6.

После блокировки пользователя происходит его оперативное отключение от Системы, текущий сеанс блокируется. При каждом новом входе в Систему необходимо ввести данные для авторизации.

9 Журналы аудита

К перечню журналов аудита относится журнал событий безопасности и журналы аудита на уровне ОС.

Журнал событий безопасности по умолчанию располагается C:\Program Data\Infomaximum\logs\security.log. Подробнее о журналах аудита на уровне ОС в п. **Ошибка! Источник ссылки не найден.**.

9.1 Размер журналов аудита Системы

Предположительный размер файлов лога системы вычисляется по формуле:

$$\text{Память в год} = \text{Количество сотрудников} * 1\ \text{Мб}^{1}$$

Файл logback.xml позволяет настраивать ротацию логов. Логи безопасности по умолчанию хранятся 3 года. Если период недостаточен, необходимо исправить файл конфигурации. Подробнее ротация логов описана в п.9.3

9.2 Описание журналов аудита

Журнал аудита предоставляется по стандартному протоколу syslog. Формат журналирования основан на спецификации: RFC 5424. Спецификация RFC 5424: https://tools.ietf.org/html/rfc5424, https://rfc2.ru/5424.rfc.

Подробнее события логирования представлены в таблицах Таблица 2,Таблица 3,Таблица 4. События, которые не логируются на данный момент в системе:

- Очистка журнала событий
- Изменение настроек аудита (включение\отключение, изменение уровня логирования)
- Копирование объекта
- Архивирование данных

[1] Формула основана на субъективных данных

- Попытка удаления журналов аудита
- Изменение конфигурации системы (конфигурационных файлов, настроек СУБД, настроек ПО)
- Остановка\сбой подсистемы (компонент, сервисов, инстансов)

Таблица 2

Спецификация полей журнала аудита

№	Описание	Комментарий	Зарезервированное значение
1	Приоритет	Все сообщения идут с одним приоритетом: 4*8+5	37
2	Версия syslog		1
3	Время события	В формате модификация RFC 3339 (с учетом требований RFC 5424)	
	HOSTNAME	Имя сервера, если определить не удалось или имя не соответствует требованиям RFC 5424, то "-"	
4			
5	Имя процесса	Нарушение спецификации. Спецификация требует указать имя приложения (java), но это не обеспечивает уникальность продукта.	infomaximum
5	ID процесса (PID)	Если pid определить не удалось, то '-'	
6	MSGID события	Уникальный идентификатор события, основан на «инкрементирующем значении». Строковое значение типа события	

Таблица 3

Структурированные данные в журнале аудита

Поле	Обязательное	Описание
Meta		
sequenceId	Да	Идентификатор события, основан на "инкременте
Система: system@729368		
version.platform	Да	Версия ядра
version.proceset	Нет	Версия proceset
Источник: source@729368		
system	Да	Внутреннее действие системы
remote_address remote_proxy	Да	Запросы без авторизации. Тип источника: «anonymous» remoteAddress - удаленный адрес, с которого пришел запрос; remoteProxy - если сервер находится за

Поле	Обязательное	Описание
		прокси, то через HTTP заголовок X-Real-IP, можно указать реальный ip;
remoteAddress remoteProxy id sessionHash login	Да	Запрос пользователя. Строковый тип источника: «employee»; remoteAddress - удаленный адрес, с которого пришел запрос; remoteProxy - если сервер находится за прокси, то через HTTP заголовок X-Real-IP, можно указать реальный ip id- ID сотрудника; sessionHash - SHA256 от строкового значения сессии; login - логин сотрудника;
remoteAddress remoteProxy id name		Запрос ключа API. Строковый тип источника: «api_key» remoteAddress - удаленный адрес, с которого пришел запрос; remoteProxy - если сервер находится за прокси, то через HTTP заголовок X-Real-IP, можно указать реальный ip; id - ID ключа API; name - название ключа API;
Объект над которым произведено действие: target@729368		
Объект: «system» (Система)		
Initialize Start Stop crush	Да	События: Initialize - Начало инициализации системы; Start - Начало работы; Stop - Окончание работы; crush - Окончание работы с ошибкой;
Объект: «employee» (Сотрудник)		
		Данные объекта сотрудник: Id – ID сотрудника; Login – логин сотрудника;
Create Update Remove Logon Logout Change_password Change_enabled_logon Adding_access_role Removing_access_to_employee	Да	Событие: Create – Создание; Update – Изменение; Remove – Удаление; Logon – Вход в систему; Logout – Выход из системы; Change_password – Смена пароля; Change_enabled_logon – Блокировка/Разблокировка сотрудников; Adding_access_role – Название роли доступа; Removing_access_to_employee – Отзыв доступа у сотрудника;
Объект: «setting» (Настройки)		
Change_complex_password Change_min_password_length Change_password_expiration_time Change_max_invalid_logon_count	Да	Событие: Change_complex_password – включение/выключение контроля сложности пароля; Change_min_password_length - Изменение минимальной длины пароля; change_password_expiration_time - Изменение времени жизни пароля; change_max_invalid_logon_count - Изменение лимитов на попытки входа в систему;

Поле	Обязательное	Описание
Объект: «access_role» (Роли доступа)		
		Данные объекта роли доступа: Id – ID сотрудника; Name – название роли доступа;
Create Update Remove Change_privilege		Событие: Create – Создание; Update – Изменение; Remove – Удаление; Change_privilege – Изменение привилегии;
Объект: «api_key» (Ключи API)		
		Данные объекта ключи API: Id – ID сотрудника; Name – название роли доступа;
Create Update Remove Change_privilege Change_access_to_report		Событие: Create – Создание; Update – Изменение; Remove – Удаление; Change_privilege – Изменение привилегии; Change_access_to_report – изменение доступа к аналитическим отчётам;
Объект: «api_key"» (База данных)		
integrity_check	Да	integrity_check – проверка целостности БД;
Объект: «integration» (Интеграция)		
logon	Да	Logon – авторизация в системе.

Таблица 3

Типы событий

Тип события	Дополнительные параметры	Описание
Событие над объектом: «employee» (Сотрудник)		
Create	first_name second_name patronymic personnel_number login email	first_name – Имя; second_name – Фамилия; patronymic personnel_number – табельный номер; login – логин; email – электронная почта;

Тип события	Дополнительные параметры	Описание
Update	old_first_name old_second_name old_patronymic old_personnel_number old_login old_email new_first_name new_second_name new_patronymic new_personnel_number new_login new_email	old_first_name - старое значение имени; old_second_name - старое значение фамилии; old_patronymic - старое значение отчества; old_personnel_number – старое значение табельного номера; old_login – старое значение логина; old_email – старое значение электронной почты; new_first_name – новое значение имени; new_second_name – новое значение фамилии; new_patronymic - новое значение отчества; new_personnel_number – новое значение табельного номера; new_login – новое значение логина; new_email – новое значение электронной почты.
Logon	status: - success - invalid_logon - disabled_logon - expired_password - invalid_logon_and_max_logon- attempts_exceed session_hash	status - Статус авторизации. Возможные значения: success – успешная; invalid_logon – неуспешная (неверные учётные данные); disabled_logon – отключен вход в систему; expired_password – срок действия пароля закончился; invalid_logon_and_max_logon – превышение количества попыток входа в систему; session_hash - хэш сессии.
Logout	cause: – timeout; – manual; – force. session_hash:	cause – Причина; Timeout – истекло время жизни сессии; Manual – пользователь разлогинился Force – система принудительно удалила сессия; session_hash - хэш сессии.
Change_password	cause – employee_update change_expiration_password; – reset_password; – set_password_by_invitation.	cause – Причина; employee_update – обновление сотрудника; change_expiration_password - смена пароля с истекшим временем жизни; reset_password – сброс пароля; set_password_by_invitation - задание пароля при переходе по ссылке из приглашения.
Change_enabled_logon	old_value: – true; – false. new_value: – true; – false.	old_value – старое значение; new_value – новое значение; true – вкл.; false – выкл.
Adding_access_role	employee_id login all: – true;	employee_id – id сотрудника; login – логин сотрудника; all – доступ ко всем сотрудникам; true – вкл.
Removing_access_to_employee	employee_id login all: – true;	employee_id – id сотрудника; login – логин сотрудника; all – доступ ко всем сотрудникам; true – вкл.
Событие над объектом: «setting» (Настройки)		

Тип события	Дополнительные параметры	Описание
Change_complex_password	old_value: - true - false new_value: - true - false	old_value – старое значение; new_value – новое значение; true – вкл; false – выкл;
Change_min_password_length	old_value: - true - false new_value: - true - false	old_value – старое значение; new_value – новое значение;
Change_password_expiration_time	old_value: new_value:	old_value – старое значение в секундах; new_value – новое значение в секундах;
Change_max_invalid_logon_count	old_value: new_value:	old_value – старое значение; new_value – новое значение;
Событие над объектом: «access_role» (Роли доступа)		
Create	name	Name – название;
Update	old_name new_name	old_name – старое название; new_name – новое название;
Remove		
Change_privilege	privivilege old_operations new_operations	Privivilege – название привилегии; old_operations – старое значение операции доступа; new_operations – новое значение операции доступа;
Событие над объектом: «api_key» (Ключ API)		
Create	name	Name – название;
Update	old_name new_name	old_name – старое название; new_name – новое название;
Remove		
Change_privilege	privivilege old_operations new_operations	Privivilege – название привилегии; old_operations – старое значение операции доступа; new_operations – новое значение операции доступа;
Change_access_to_report	old_reports new_reports	old_reports – старый доступ к отчётам; new_reports – новый доступ к отчётам;
Событие над объектом: «database» (База данных)		
Integrity_check	Status*:* -success -fail	Status - статус success – успешно; fail – не успешно;
Событие над объектом: «integration» (Интеграция)		
logon	Status*:* -success -fail	Status - статус success – успешно; fail – не успешно;

События «попытки несанкционированного доступа к Системе» не логируются, т.к. защита от несанкционированного доступа производится на уровне файловой системы.

Логирование «результатов контроля целостности АС контроля работоспособности СЗИ» не осуществляется. Также не осуществляется подсчёт данных хеша в конфигурационном файле, так как подсчёт данных не гарантирует их сохранность от изменений. Защита может осуществляться только на уровне файловой системы.

Формат записи:

```
37<1> <time> <hostname> infomaximum <pid> <MSGID> 2]meta sequenceId=""]
[system@729368 version.core="1.0.0" version.proceset="1.0.0"][source@729368 ...]
[event@729368 ...][target@729368 ...]
```

Пример записи в журнале аудита:

```
<37>1~2019-03-26T16:07:06+03:00~infomaximum61~infomaximum~9160~update~[meta
sequenceId="80"]~[system@729368 version.platform="1.0.0" version.proceset="1.0.0
"]~[source@729368 sessionHash="3915d830623a26b61a044d1ad9c1bebb6e61705a969559e1c
5f436d2210aabcc" id="1" type="employee" login="admin" remoteAddress="10.0.75.1"]
~[event@729368 old_first_name="Денис" old_email=petr@gmail.com new_first_name="В
ладимир" new_email="email@gmail.com"]~[target@729368 module="platform"    id="2"
type="employee" login="vpetrov"]
```

Таблица 4

Таблица соответствие видов событий журнала

Информация о событие в терминах ДЗИ	**Элемент в строке в журнале аудита**	**Примечание**
Уникальный номер строки о событии ИБ	[meta sequenceId="80"]	Значение meta sequenceId является уникальным номером строки о событии.
Название АС-источника информации о событии	[source@729368 … type="employee"…]	Значение type в source является типом источника события. Подробнее в Таблица *2*.
Версия источника информации о событии	[system@729368 version.platform= "1.0.0" version.proceset="1.0.0"]	Значение version.platform и version.proceset является информации о источнике события. Подробнее в таблице 3.
Системное имя (логин) пользователя-инициатора события	[source@729368 … id="1" type="employee" login="admin"…]	Значение id="1", " login="admin" являются информации о пользователи-инициаторе, а именно login – логин, id – порядковый номер пользователя; Подробнее в Таблица 2.
IP адрес хоста-источника события	[source@729368… remoteAddress= "10.0.75.1"]	Значение remoteAddress является IP адресом хоста-источника события.
Системное имя (логин) пользователя получателя	[target@729368 …id="1" type="employee" login="admin"]	Значение в target id="1" type="employee" login="admin" являются информацией о пользователе-получателе, где id – порядковый номер сотрудника,login – логин сотрудника, type – это тип получателя.
Системный идентификатор сообщения о событии	update	Идентификатором сообщением о событии может быть значение <MSGID> , подробнее в Таблица 2.
Системное время источника события	2019-03-26T16:07:06+03:00	Время источника события фиксируется в строке под <time>. Формат даты: yyyy-MM-ddTHH:mm:ssZ

Текст сообщения в максимально подробном виде, включая старые и новые значения измененных свойств;	[event@729368 old_first_name="Денис" old_email=petr@gmail.com new_first_name="Владимир" new_email="email@gmail.com]	Где old_first_name – старое значение имени, old_email – старое значение электронного адреса, new_first_name – новое значение имени, new_email – новое значение электронной почты. Подробнее в Таблица 3.
Полное имя процесса (службы); результат (успех/отказ).		Результат успех/отказ фиксируется не для всех событий в Системе. Подробнее в Таблица 3.

9.3 Ротация журнала аудита

Все журналирование системы основано на компоненте Logback. (https://logback.qos.ch/)
По умолчанию, в Системе применяется файл конфигурации: C:\ProgramData\Infomaximum\logback.xml. Так же в Системе возможны варианты с переопределением файла конфигурации, используя механизм приоритезации загрузки файла конфигурации.

Подробно о формате файла конфигурации, а также о приоритетах загрузки файлов конфигурации, можно посмотреть в документации:
https://logback.qos.ch/manual/configuration.html

По умолчанию в системе включена ротация логов, для журнала безопасности применяются следующие правила: файл журнала аудита упаковывается в архив и переименовывается в соответствии с шаблоном (`"security.%d{yyyy-MM-dd}.%i.log.gz`") при следующих условиях:

- Наступили следующие сутки
- Журнал лога превысил размер в 50 Мб

По умолчанию, файлы журнала безопасности хранятся 3 года. по истечению этого времени старые журналы безопасности удаляются. Параметры, которые отвечают за ротацию логов настраиваются в файле: logback.xml. Путь файла: C:\ProgramData\Infomaximum

9.3.1 Горячее обновление конфигурации

В системе, по умолчанию предусмотрен механизм "горячего" обновления конфигурации, за это отвечают параметры «scan" и «scanPeriod". По сканирование происходит каждые 30 секунд. Соответственно этот механизм позволяет временно изменять правила логирования, в плоть до полного его отключения. (`<configuration scan="true" scanPeriod="30 seconds">`)