Учебно-лабораторный стенд на базе отечественного ПО MasterSCADA 4D. Функции информационной безопасности в версии Enterprise

Часть 2

Александр Гаврилов (КПФУ, ИНСТИТУТ ФИЗИКИ), Александр Деркач («РЕГИОН-ПРОФ» «ПРОСОФТ КАЗАНЬ»), Ольга Киселёва (ПРОСОФТ), Андрей Лытаев (КПФУ, ИНСТИТУТ ФИЗИКИ), Вячеслав Маценко («РЕГИОН-ПРОФ» «ПРОСОФТ КАЗАНЬ»)

Специалист по информационной безопасности (ИБ) – в настоящее время одна из наиболее востребованных IT-специальностей. В том числе этому способствуют требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры РФ. В этой статье изложена концепция развития учебно-лабораторного комплекса, созданного в Институте Физики Казанского (Приволжского) федерального университета совместно со специалистами компании «Прософт». Описание комплекса было приведено в журнале СТА № 4 за 2024 год. Рассматриваются вопросы, связанные с обеспечением ИБ на промышленных объектах. Особое внимание уделено рассмотрению руководящих документов и мер защиты, используемых в области ИБ АСУ ТП. В статье сделан обзор функций информационной безопасности, входящих в состав ПО MasterSCADA 4D версии Enterprise.

Авторы благодарят компанию МПС софт и лично руководителя отдела защиты информации и безопасной разработки ПО Константина Викторовича Белошапко за предоставленные материалы, идеи и поддержку.

Введение

Эффективное обеспечение информационной безопасности промышленных объектов требует комплексного подхода, включающего в себя следование требованиям нормативно-правовых документов, реализацию мер защиты организационного и технического характера на разных уровнях АСУ ТП.

Такой системный подход применим и на учебном стенде, для обучения по дисциплинам «Технология построения защищённых автоматизированных систем», «Экспертные системы комплексной оценки безопасности автоматизированных информационных и телекоммуникационных систем», «Технология обеспечения информационной безопасности объектов», «Управление информационной безопасностью» и т.д. Изучение этих дисциплин возможно проводить по следующему сценарию:

- краткий обзор государственных стандартов и федеральных законов в области обеспечения ИБ в промышленных системах автоматизации;
- изучение особенностей АСУ ТП как объекта кибератак (объекты защиты, источники угроз, векторы атак);
- рассмотрение мер ИБ-защиты АСУ ТП, регламентированных нормативно-правовыми документами;
- получение практических навыков в области ИБ с применением средств защиты, входящих в состав программных и аппаратных компонентов системы автоматизации;
- применение специализированных наложенных средств защиты информации (СЗИ).

Изложенная выше концепция проиллюстрирована на рис. 1. Рассмотрим детальнее основные её части.

Краткий обзор стандартов и федеральных законов в области ИБ АСУ ТП

В Российской Федерации обеспечение ИБ АСУ ТП регламентируется Федеральным законом № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», приказами ФСТЭК России от 14.03.2014 № 31, от 21.12.2017 № 235, от 22.12.2017 № 236, от 25.12.2017 № 239 и Указом Президента РФ от 30.03.2022 № 166 по обеспечению

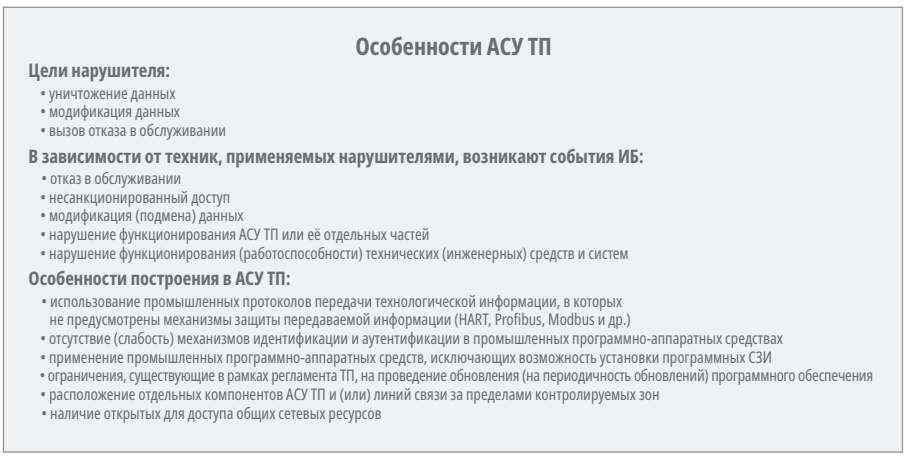
Рис. 1. Концепция учебно-лабораторного стенда «Информационная безопасность в АСУ ТП»

технологической независимости. Также в области информационной безопасности промышленных систем автоматизации существует ряд международных стандартов, в том числе серия стандартов IEC 62443. Ряд этих стандартов были гармонизированы в России.

Описанные в данных нормативных документах требования к обеспечению защиты информации и соответствующие меры защиты могут быть использованы в разных системах промышленной автоматики. Инциденты нарушения информационной безопасности возможны в любых промышленных системах автоматизации. Таким образом, данные документы необходимо рассматривать как методические при изучении основ построения защищённых АСУ ТП.

Изучение особенностей информационной безопасности АСУ ТП

Анализ рисков, связанных с уязвимостью технологических решений на объектах АСУ ТП, можно начать с отчёта ФСТЭК России (Федеральная служба по техническому и экспортному контролю) от 3 октября 2024 года «Реализация законодательства ОБ КИИ. Реализация технических мер по повышению защищённости. Особенности АСУ ТП» (рис. 2). В нём учтены в том числе и международные практики, которые показывают, что промышленные протоколы передачи технологической информации строились без учёта специфики информационной безопасности – в них нет механизмов защиты передаваемой информации (HART, Profibus, Modbus и др.), отсутствуют или слабо представлены механизмы идентификации и аутентификации. Особо следует обратить внимание на обновления программного обеспечения. Например, во многих широко известных SCADA-системах по умолчанию используются сервисы, которые об-



Особенности АСУ ТП

Цели нарушителя:
- уничтожение данных
- модификация данных
- вызов отказа в обслуживании

В зависимости от техник, применяемых нарушителями, возникают события ИБ:
- отказ в обслуживании
- несанкционированный доступ
- модификация (подмена) данных
- нарушение функционирования АСУ ТП или её отдельных частей
- нарушение функционирования (работоспособности) технических (инженерных) средств и систем

Особенности построения в АСУ ТП:
- использование промышленных протоколов передачи технологической информации, в которых не предусмотрены механизмы защиты передаваемой информации (HART, Profibus, Modbus и др.)
- отсутствие (слабость) механизмов идентификации и аутентификации в промышленных программно-аппаратных средствах
- применение промышленных программно-аппаратных средств, исключающих возможность установки программных СЗИ
- ограничения, существующие в рамках регламента ТП, на проведение обновления (на периодичность обновлений) программного обеспечения
- расположение отдельных компонентов АСУ ТП и (или) линий связи за пределами контролируемых зон
- наличие открытых для доступа общих сетевых ресурсов

Рис. 2. Слайд из презентации ФСТЭК России от 3 октября 2024 года, отчёт «Реализация законодательства ОБ КИИ. Реализация технических мер по повышению защищённости. Особенности АСУ ТП»

Рис. 3. Обобщённое представление угроз безопасности АСУ ТП, в соответствии с БДУ ФСТЭК

ращаются в сеть Интернет для своевременного обновления. При технологическом импортозамещении стоит учитывать эти факторы и вводить применение дополнительных мер по защите.

Критически важные компоненты, нарушение которых может привести к негативным последствиям для технологического процесса, являются объектами защиты в автоматизированной системе управления.

ФСТЭК России размещает актуальные сведения об уязвимостях и угрозах информационной безопасности в АСУ ТП на специальном ресурсе, имеющем название Банк данных угроз (БДУ) АСУ ТП [1]. В соответствии с представлением на сайте (рис. 3) и пользовательским

Таблица 1. Типы и группы компонентов объектов воздействия в соответствии с БДУ АСУ ТП

Тип компонента	Группы компонентов
К.1 Программное обеспечение	К.1.1 Микропрограммное обеспечение
	К.1.2 Системное ПО
	К.1.3 Сервисное ПО
	К.1.4 Инструментальное ПО
	К.1.5 Прикладное ПО
	К.1.6 Программное средство защиты информации
	К.1.7 Веб-приложение
	К.1.8 Специальное ПО
К.2 Программно-аппаратные средства	К.2.1 Периферийное оборудование
	К.2.2 Интерфейсы ввода/вывода
	К.2.3 Устройство хранения данных
К.3 Сетевые компоненты	К.3.1 Канал передачи данных
	К.3.2 Протокол передачи данных
К.4 Пользователи	К.4.1 Привилегированные пользователи

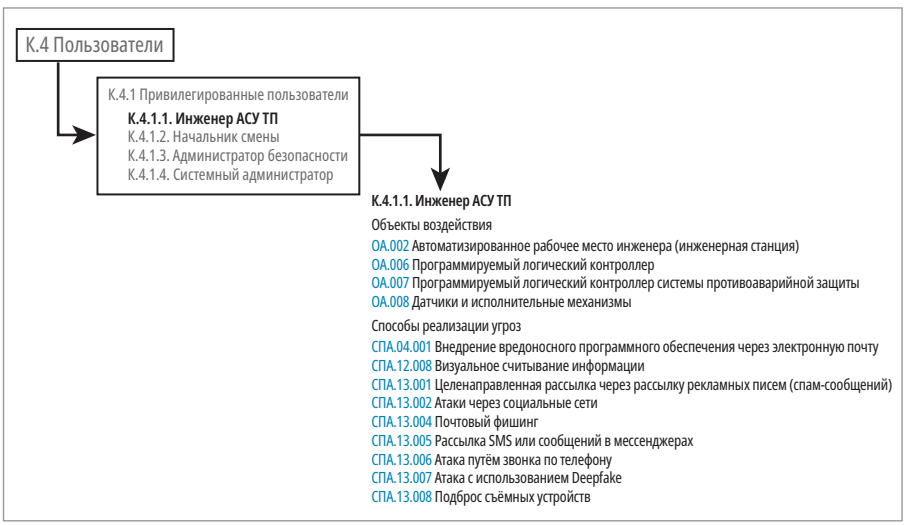


Рис. 4. Информационная карточка компонента «К.4.1.1. Инженер АСУ ТП» в соответствии с БДУ ФСТЭК

соглашением ресурса данная информация представляет собой обобщённый перечень основных угроз безопасности информации, потенциально опасных для АСУ ТП. Объекты воздействия определяются в БДУ АСУ ТП следующим списком [2]:

ОА.001 Автоматизированное рабочее место оператора (диспетчера)

ОА.002 Автоматизированное рабочее место инженера (инженерная станция)

ОА.003 Промышленный сервер

ОА.004 Сервер архивов

ОА.005 Панель оператора

ОА.006 Программируемый логический контроллер

ОА.007 Программируемый логический контроллер системы противоаварийной защиты

ОА.008 Датчики и исполнительные механизмы

ОА.009 Съёмный носитель информации

ОА.010 Устройство промышленного Интернета вещей

ОА.011 Активное сетевое оборудование

ОА.012 Средства защиты информации

ОА.013 Мобильное устройство

Каждый из указанных объектов воздействия имеет один или несколько компонентов, в направлении которых могут быть направлены векторы информационной атаки. Типы и группы компонентов объектов воздействия приведены в обобщённой табл. 1. С более детальным их описанием можно ознакомиться на сайте БДУ АСУ ТП.

В качестве примера на рис. 4 в наглядном виде представлено описание группы «К.4.1 Привилегированные пользователи». По информационной карточке «К.4.1.1. Инженер АСУ ТП», расположенной на сайте регулятора [3], можно определить, в какие объекты воздействия он может входить, ознакомиться с потенциальными способами реализации угроз для этого компонента, а также определить возможные меры защиты.

Меры ИБ-защиты АСУ ТП

С чего начинать построение системы защиты? Эксперты [4] отмечают, что первый этап может быть самым простым и доступным, поэтому первоочередные мероприятия заключаются в настройке встроенного в АСУ ТП функционала безопасности: механизмов контроля и управления доступом, регистрации и учёта, резервного копирования настроек и данных, средств обеспечения сетевой безопасности и т.д.

Этот же тезис подчёркивается и в приказе № 31 ФСТЭК: в качестве средств защиты информации в первую очередь подлежат рассмотрению механизмы защиты (параметры настройки) штатного программного обеспечения автоматизированной системы управления.

В табл. 2 приведены группы мер защиты, определённые приказами ФСТЭК № 31 и № 239. С перечнем мер защиты внутри каждой группы можно ознакомиться в первоисточниках, т.е. непосредственно в этих документах, опубликованных на сайте ФСТЭК [5, 6].

Кроме того, на ресурсе БДУ АСУ ТП ФСТЕК для каждой меры защиты [7] опубликована информационная карточка, содержащая:

- описание меры;
- перечень потенциальных блокируемых угроз безопасности информации;
- блокируемые способы реализации угроз.

Функции информационной безопасности в версии MasterSCADA 4D Enterprise

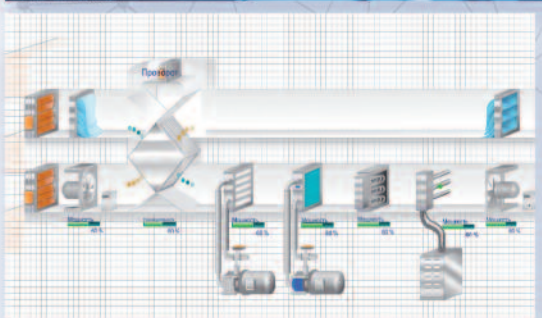
Разработчики пакета программ MasterSCADA 4D включили в программное обеспечение набор инструментов, позволяющих реализовать средствами пакета некоторые меры защиты, определённые приказами ФСТЭК № 31 и № 239 (табл. 2). В частности, хорошо представлен инструментарий для групп:

- I Идентификация и аутентификация (ИАФ);
- II Управление доступом (УПД);
- V Аудит безопасности (АУД);
- VIII Обеспечение целостности (ОЦЛ);

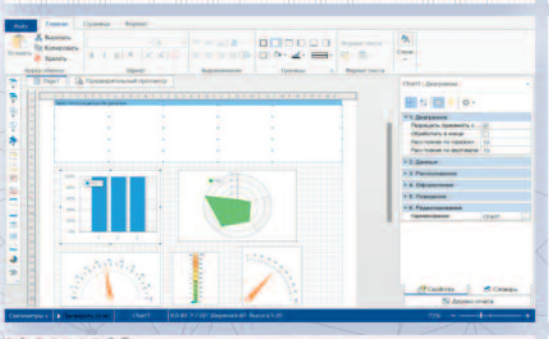
MasterSCADA

MasterSCADA 4D — российская программная платформа для разработки систем автоматизации и диспетчеризации в различных отраслях промышленности

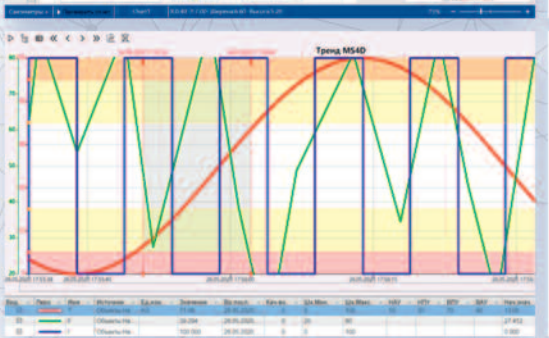
Внесена в реестр отечественного ПО № 13907



Визуализация технологического процесса



Формирование и выдача отчетов



Хранение истории контролируемых параметров

Таблица 2. Группы мер защиты, определённые приказами ФСТЭК № 31 и № 239

	Наименование группы мер защиты	Подгруппы
I	Идентификация и аутентификация (ИАФ)	ИАФ.0...ИАФ.7
II	Управление доступом (УПД)	УПД.0...УПД.14
III	Ограничение программной среды (ОПС)	ОПС.0....ОПС.3
IV	Защита машинных носителей информации (ЗНИ)	ЗНИ.0...ЗНИ.8
V	Аудит безопасности (АУД)	АУД.0...АУД.11
VI	Антивирусная защита (АВЗ)	АВЗ.0...АВЗ.5
VII	Предотвращение вторжений (компьютерных атак) (СОВ)	СОВ.0...СОВ.2
VIII	Обеспечение целостности (ОЦЛ)	ОЦЛ.0...ОЦЛ.6
IX	Обеспечение доступности (ОДТ)	ОДТ.0...ОДТ.8
X	Защита технических средств и систем (ЗТС)	ЗТС.0...ЗТС.6
XI	Защита информационной (автоматизированной) системы и её компонентов (ЗИС)	ЗИС.0...ЗИС.39
XII	Реагирование на компьютерные инциденты (ИНЦ)	ИНЦ.0...ИНЦ.6
XIII	Управление конфигурацией (УКФ)	УКФ.0...УКФ.4
XIV	Управление обновлениями программного обеспечения (ОПО)	ОПО.0...ОПО.4
XV	Планирование мероприятий по обеспечению безопасности (ПЛН)	ПЛН.0...ПЛН.2
XVI	Обеспечение действий в нештатных ситуациях (ДНС)	ДНС.0...ДНС.6
XVII	Информирование и обучение персонала (ИПО)	ИПО.0...ИПО.4

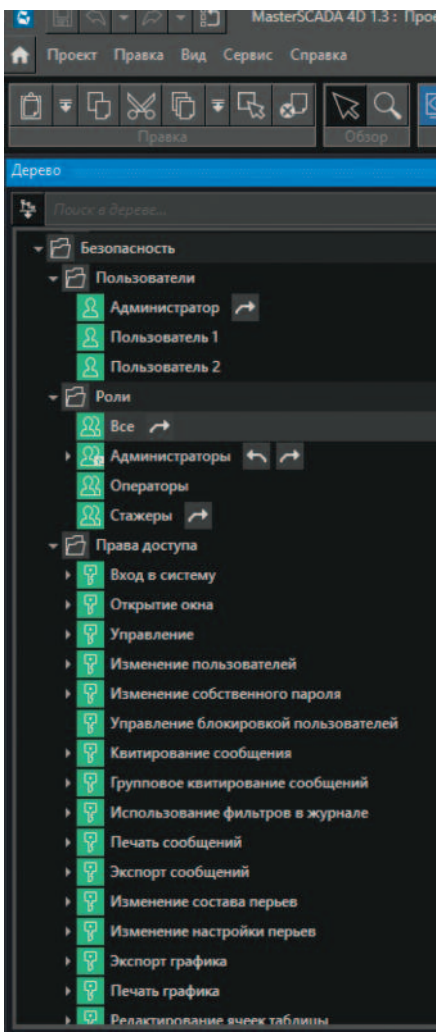


Рис. 5. Группа «Безопасность» дерева проекта ***(рисунки здесь и далее касаются проекта в среде разработки MasterSCADA4D)***

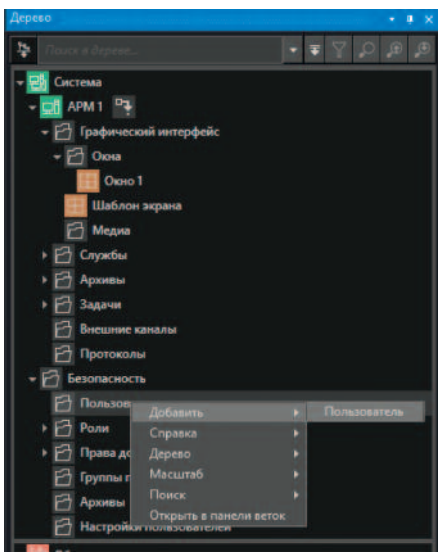


Рис. 6. Создание нового пользователя

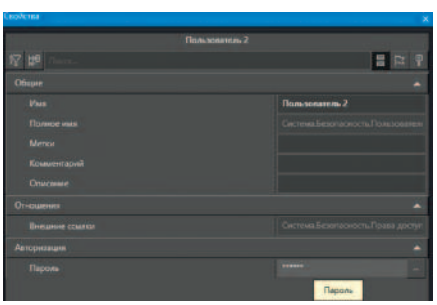


Рис. 7. Панель свойств пользователя

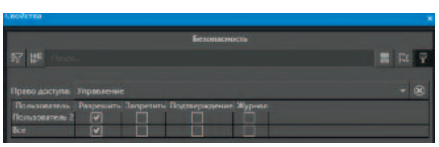


Рис. 8. Панель редактирования прав доступа

- XI Защита информационной (автоматизированной) системы и её компонентов (ЗИС).

Ряд базовых мер защиты вводится в проект путём настроек элементов группы «Безопасность» дерева проекта (рис. 5).

Это создание учётных записей пользователей, создание и настройка ролей, настройка прав доступа и т.п. Этот набор мер может быть обогащён путём использования встроенных в MasterSCADA 4D библиотечных функциональных блоков (ФБ). Встроенные ФБ позволяют: создавать, контролировать, модифицировать учётные записи на этапе исполнения проекта; создавать и модифицировать роли на этапе исполнения проекта и т.п. Далее кратко опишем ряд встроенных возможностей пакета MasterSCADA 4D по реализации мер защиты. Это описание нисколько не претендует на детальное изложение вопроса.

Полное описание функций ПО содержится в руководстве по эксплуатации и онлайн-справке [8]. Наша задача – соотнести текущие возможности пакета MasterSCADA 4D с требованиями регулятора и рекомендовать инженерам использование этих возможностей на практике.

Идентификация и аутентификация

Создание учётных записей на этапе разработки проекта

В MasterSCADA 4D основные опции ИБ сосредоточены в группе «Безопасность» дерева проекта (рис. 5). Здесь, в разделе «Пользователи», можно добавить в проект нового пользователя (рис. 6), назначить ему в панели свойств пароль (необязательно) (рис. 7) и установить права доступа (рис. 8). Если была создана хотя бы одна учётная запись пользователя, в момент подключения клиента к среде исполнения на экране клиентского приложения появляется диалог «Вход в систему» с предложением выбрать пользователя и ввести пароль (рис. 9).

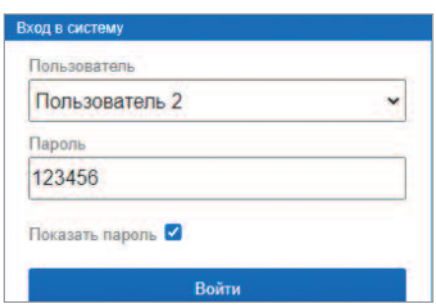


Рис. 9. Диалог «Вход в систему»

Таблица 3. Функциональные блоки управления учётными записями пользователей

ФБ UsersGet	Получение списка пользователей, локально для каждого узла
ФБ UsersAdd	Добавление пользователей в RT, пользователь добавится в узел, на котором исполняется ФБ
ФБ UsersSetGroup	Назначение/изменение списка ролей пользователя
ФБ UsersDelete	Удаление пользователя, ранее добавленного в режиме исполнения
ФБ UsersGetGroups	Получение списка ролей, в которые добавлен пользователь
ФБ UsersSetPassword	Назначение/изменение пароля пользователя, ранее добавленного в режиме исполнения
ФБ UsersRename	Изменение имени существующего пользователя. При переименовании пользователя сохраняются его назначение на роли и пароль
(тип Enterprise)	Тип для экземпляров ФБ, позволяющий получать значения дополнительных настроек пользователей, заданных разработчиком проекта. Например, дата рождения, должность, длина пароля, срок действия пароля и т.д. Enterprise
ФБ UsersSetSettings (тип Enterprise)	Тип для экземпляров ФБ, позволяющий изменять значения дополнительных настроек пользователей, заданных разработчиком проекта. Например, дата рождения, должность, длина пароля, срок действия пароля и т.д. Enterprise

Создание учётных записей на этапе исполнения проекта

Дополнительную гибкость управления учётными записями пользователей на этапе исполнения проекта предоставляют встроенные в среду разработки функциональные блоки (табл. 3). Они позволяют добавлять и удалять новых пользователей, изменять имя и пароль пользователя и т.п. Например, на рис. 10 показан диалог добавления новых и удаления существующих учётных записей пользователей на этапе исполнения, реализованный с применением ФБ UsersAdd и UsersDelete.

В результате работы ФБ UsersAdd создаётся файл Users – уникальный GUID проекта внутри рабочей папки исполнительной системы. Файл содержит записи данных новых пользователей. Файл закодирован. Взамен файла Users можно использовать внешнюю базу данных PostgreSQL.

Интеграция с Active Directory и LDAP

В MasterSCADA 4D можно объединить встроенную систему безопасности и базы данных службы каталогов двух типов:

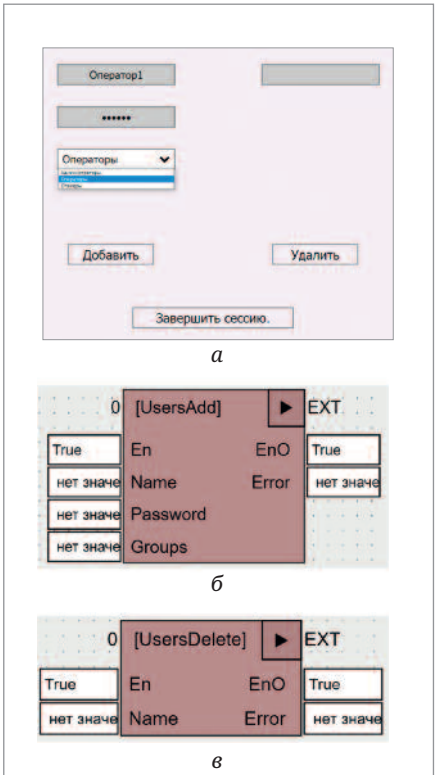
- Active Directory Windows – для тех проектов MasterSCADA 4D, где используется среда исполнения, расположенная на устройстве с ОС Windows;
- службы каталогов, основанных на использовании кроссплатформенного протокола LDAP (Lightweight Directory Access Protocol) – для тех проектов MasterSCADA 4D, где используется среда исполнения, расположенная на устройстве с ОС Linux.

Соответствующие настройки для использования такого способа идентификации пользователей в проекте показаны на рис. 11.

Установление характеристик пароля, устойчивых к перебору

Политика управления паролями связана со следующими настройками безопасности в проекте MasterSCADA 4D (рис. 12).

- **Минимальная длина пароля.** Определяется минимальное количество символов при настройке пароля в режиме исполнения.
- **Количество неповторяемых паролей.** Указывает, сколько раз пользователь должен задать неповторяющийся пароль. Если указано значение 0, то ограничения отсутствуют.
- **Использовать сложный пароль.** Определяет состав символов при настройке пароля в режиме исполнения. Если флаг установлен, то пароль должен содержать хотя бы одну цифру, одну прописную и одну строчную букву.
- **Пароль должен содержать спецсимвол.** Определяет наличие спецсимвола в пароле. Примеры спецсимволов: ~!@#$%^&*()—_+={}[]/\|:;'"<>,.?.
- **Срок действия пароля.** Определяет срок действия пароля пользователя. Если время действия текущего пароля достигло указанного, то при начале очередной сессии пользователя появится сообщение, и пользователь не будет допущен к работе до тех пор, пока пароль не будет изменён в режиме исполнения.



а

б

в

Рис. 10. Диалог добавления и удаления учётных записей пользователей на этапе исполнения (а), реализованный с применением ФБ UsersAdd (б) и UsersDelete (в)

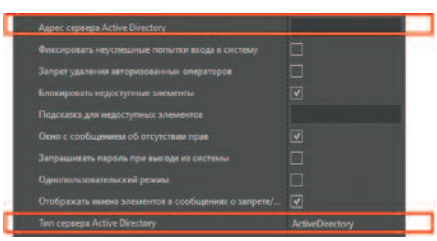


Рис. 11. Окно свойства группы «Безопасность» для настройки работы со службами каталогов Active Directory

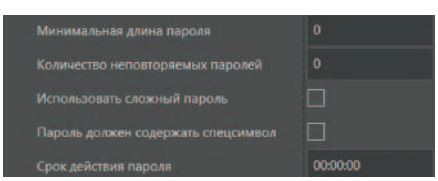


Рис. 12. Свойства группы «Роли» элемента «Безопасность» для использования паролей, устойчивых к перебору

Управление доступом

В состав мер по обеспечению безопасности, определённых приказами ФСТЭК № 31 и № 239, входит группа мер защиты информации «Управление доступом» (УПД). Эффективные инструменты для реализации ряда мер УПД включены разработчиками в состав пакета MasterSCADA 4D:

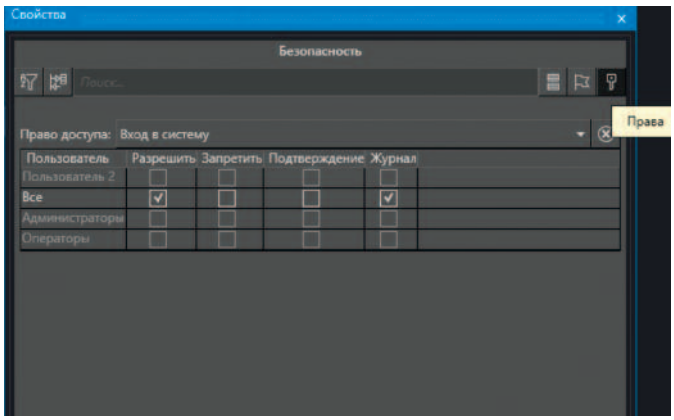


Рис. 13. Сводная таблица разрешений (прав доступа)

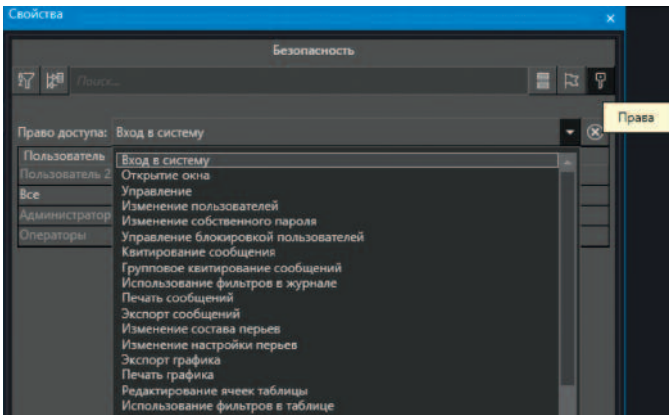


Рис. 14. Список настраиваемых прав

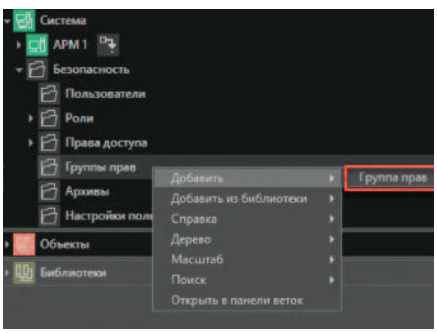


Рис. 15. Диалог добавления группы прав

Таблица 4. Функциональные блоки управления ролями

UsersRoleAdd	Служит для добавления ролей пользователей и их настроек в режиме исполнения
UsersRoleDelete	Служит для удаления ролей пользователей и их настроек в режиме исполнения
UsersGetAllRoles	Служит для получения списка ролей пользователей в режиме исполнения
UsersGetRoleSettings	Служит для получения настроек роли пользователей в режиме исполнения
UsersSetRoleSettings	Служит для изменения настроек роли пользователей в режиме исполнения
UsersSetRoleControlRight	Служит для изменения прав доступа к элементу в режиме исполнения
UsersGetRoleControlRight	Служит для получения назначенных прав доступа для роли к элементу

- УПД. 1 Управление учётными записями пользователей;
- УПД. 2 Реализация модели управления доступом;
- УПД. 4 Разделение полномочий (ролей) пользователей;
- УПД. 5 Назначение минимально необходимых прав и привилегий;
- УПД. 6 Ограничение неуспешных попыток доступа в информационную (автоматизированную) систему;
- УПД. 9 Ограничение числа параллельных сеансов доступа
- УПД. 10 Блокирование сеанса доступа пользователя при неактивности

Коротко остановимся на этих инструментах.

Модели управления доступом

В группе «УПД.2 Реализация модели управления доступом» перечислены три рекомендованные регулятором модели управления доступом: дискреционная, ролевая, мандатная.

Реализация дискреционной модели управления доступом предусматривает управление доступом субъектов доступа к объектам доступа на основе идентификационной информации субъекта и для каждого объекта доступа – списка, содержащего набор субъектов доступа (групп субъектов) и ассоциированных с ними типов доступа.

Реализация ролевой модели управления доступом предусматривает управление доступом субъектов доступа к объектам доступа на основе ролей субъектов доступа (совокупность действий и обязанностей, связанных с определённым видом деятельности).

Реализация мандатной модели управления доступом предусматривает управление доступом субъектов доступа к объектам доступа на основе сопоставления классификационных меток каждого субъекта доступа и каждого объекта доступа, отражающих классификационные уровни субъектов доступа и объектов доступа, являющиеся комбинациями иерархических и неиерархических категорий.

В MasterSCADA 4D предусмотрена комбинация дискреционной и ролевой моделей управления доступом с явным акцентом на ролевой. Остановимся на деталях реализации.

Права доступа

Настраивать права доступа для пользователей в MasterSCADA 4D можно как индивидуально, так и для группы пользователей (ролей).

Таблица для просмотра и редактирования прав доступа отдельных пользователей и ролей доступна в панели «Свойств» группы «Безопасность» дерева проекта (рис. 13, 14). Для доступа к таблице необходимо переключиться в режим просмотра прав доступа. В выпадающем списке содержится перечень доступных к настройке прав. Для предотвращения случайных нажатий необходимо установить флаг в столбце «Подтверждение». Тогда в режиме исполнения, прежде чем выполнится изменение связанного параметра, появится диалоговое окно. Для фиксации выполненных действий пользователей необходимо установить флаг в столбце «Журнал».

Для придания большей гибкости механизму назначения прав разработчики предусмотрели добавление в проект группы прав. Группы прав позволяют переопределять право «Управление» для графических элементов из катего-

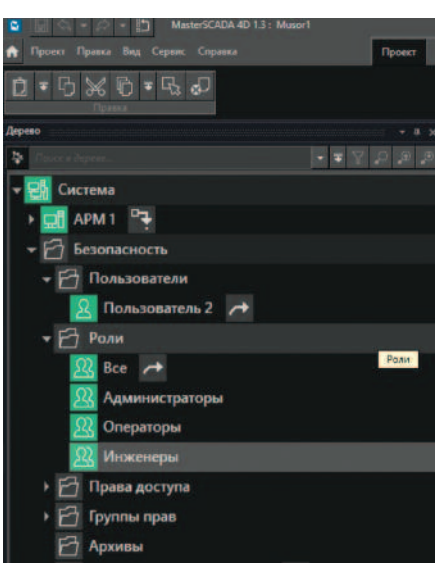


Рис. 16. Группа «Роли» дерева проекта

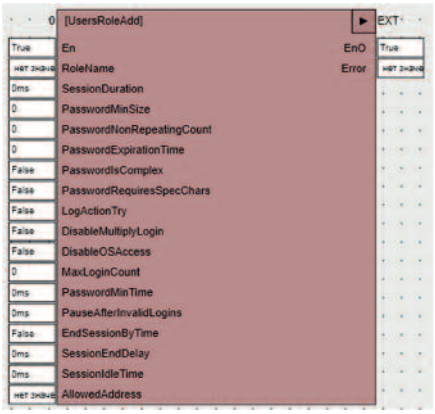


Рис. 17. ФБ UsersRoleAdd

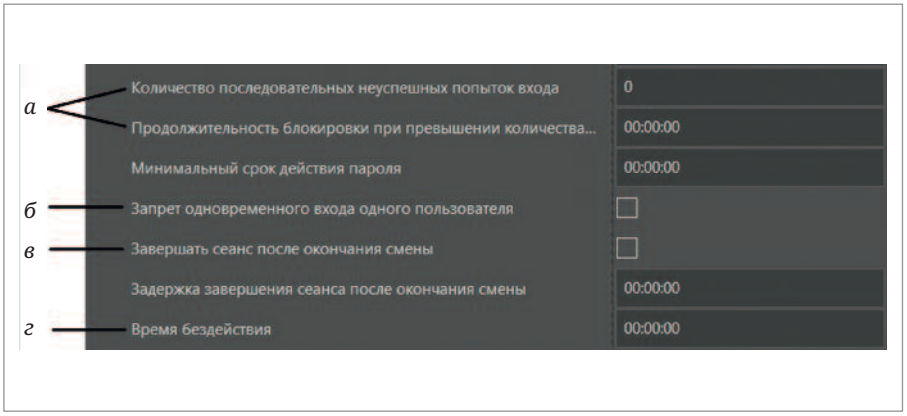


Рис. 18. (а, б, в, г) Свойства группы «Роли» для группы мер «Управление доступом»

рии «Диалог», таких как кнопки, текстовый ввод и т.д. После назначения группы прав на графический элемент право «Управление» перестаёт действовать на него, и начинает действовать группа прав (рис. 15).

Ролевая модель управления доступом

Наиболее полно в MasterSCADA 4D реализована ролевая модель управления доступом. Как правило, роли пользователей создаются для того, чтобы разделить пользователей проекта, работающих в режиме исполнения, по категориям, например: операторы, инженеры, начальники смен и т.п.

Роли создаются и модифицируются в основном на этапе разработки проекта. В группе «Безопасность» для этого существует подгруппа «Роли» (рис. 16). Для лицензии Enterprise возможно создание ролей в режиме исполнения с помощью программирования встроенных библиотечных функциональных блоков (табл. 4).

Например, на рис. 17 изображён вид в редакторе ФБД функционального блока UsersRoleAdd, который служит для добавления ролей пользователей и их настроек в режиме исполнения.

Ограничение неуспешных попыток доступа в систему

Меру защиты, связанную с ограничением неуспешных попыток доступа, можно реализовать соответствующими настройками свойств группы «Роли» элемента «Безопасность» (рис. 18, а).

Количество последовательных неуспешных попыток входа. Определяет, сколько раз пользователь может попытаться неуспешно начать сессию в клиенте визуализации.

Если установлено значение 0, то ограничение отсутствует. Данная настройка применяется только к пользователям, созданным в режиме исполнения.

Продолжительность блокировки при превышении количества неуспешных попыток входа. Определяет интервал времени, в течение которого пользователь, который не смог авторизоваться за количество попыток, разрешённое в предыдущем пункте, не сможет повторить попытки авторизоваться в клиенте визуализации.

Ограничение числа параллельных сеансов доступа

Возможность авторизоваться и запустить параллельные сеансы с нескольких клиентов визуализации определяется настройкой «Запрет одновременного входа одного пользователя» (рис. 18, б). Если флаг установлен, то возможны следующие варианты.

- В случае если есть активная сессия для этого пользователя с того же самого адреса, то закрывается прошлая сессия, создаётся новая.
- Если текущая сессия запущена на другом устройстве, с другим адресом, то в случае, если она неактивна больше 10 секунд, она закрывается и создаётся новая. Если от клиента визуализации продолжают приходить запросы к исполнительной системе, то возвращается ошибка авторизации.

Предоставление пользователям прав доступа к объектам доступа, основываясь на задачах, решаемых пользователями

Предоставление пользователям прав доступа к системе для выполнения определённых задач можно ограничить временем смены. Авторизация пользователя будет возможна только в отрезок времени, заданный по каждому дню недели. Сессия будет завершена после окончания смены, что активируется при установлении флага настройки «Завершать сеанс после окончания смены» (рис. 18, в). Время начала и конца смены по дням недели задаётся входным параметром – массивом структур TimeIntervals в ФБ UsersSetAllowedTime (рис. 19).

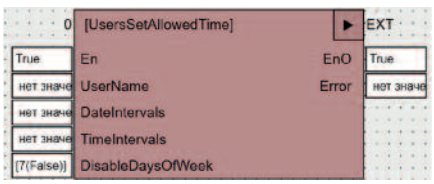


Рис. 19. ФБ UsersSetAllowedTime

Блокирование сеанса доступа пользователя при неактивности

Интервал времени, по истечении которого происходит завершение сессии, если пользователь не совершает никаких действий в окне (клики мыши, клавиатурный ввод), определяется настройкой «Время бездействия» (рис. 18, г).

Обеспечение целостности

Контроль целостности программного обеспечения

Параметры проверки целостности программного обеспечения задаются в процессе разработки проекта MasterSCADA 4D в панели свойств элемента «Безопасность». Для активации соответствующих функций требуется установить флажок в один или несколько полей следующих настроек.

- **Контроль целостности проекта.** Если флаг установлен, то в конфигурацию проекта включается файл cfg_files.dat, зашифрованный списком MD5 контрольных сумм всех загружаемых из среды разработки файлов конфигурации узла.
- **Блокировать запуск при неуспешной проверке проекта.** Определяет порядок работы при неуспешной проверке проекта. Если флаг установлен и при старте режима исполнения най-

Рис. 20. ФБ FileIntegrityControl

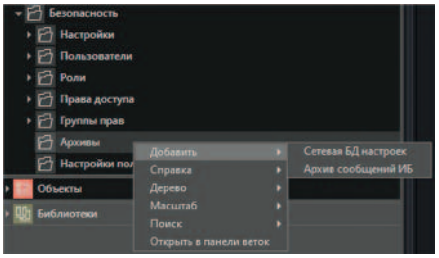


Рис. 21. Создание «Архива сообщений» ИБ

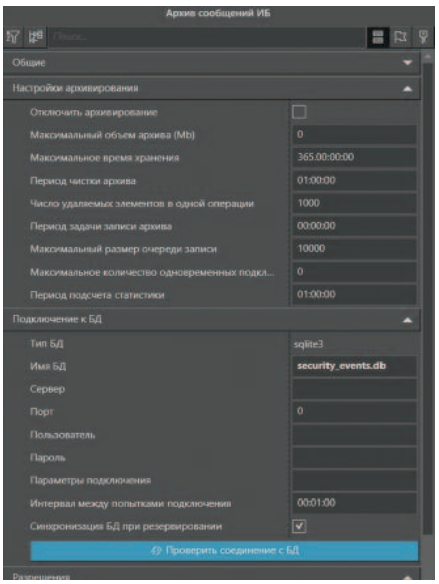


Рис. 22. Панель свойств элемента «Архив сообщений» группы «Безопасность»

дено отличие контрольных сумм файлов от прописанных в cfg_files.dat, то возникает ошибка запуска узла.

- **Период проверки целостности проекта.** Определяет период, с которым будет происходить дополнительный контроль целостности после старта режима исполнения.
- **Контроль целостности ПО.** Активирует контроль целостности программных файлов исполнительной системы.
- **Блокировать запуск при неуспешной проверке ПО.** Если флаг установлен, то исполнительная система не запустится.
- **Период проверки целостности ПО.** Определяет период, с которым будет происходить дополнительный контроль целостности после старта режима исполнения.

Для управления контролем целостности ПО или проекта, а также получения списка отличий используется Функциональный блок FileIntegrityControl (рис. 20).

Его входной параметр «CheckType» может принимать два значения: Project (выполняется проверка целостности проекта) или System (выполняется проверка целостности исполнительной системы).

Выходной параметр «FileInfo» выдаёт описание по каждому проверяемому файлу. Данный выход представляет собой массив структур, которые содержат поля: FileName – имя проверяемого файла, CheckSumFlag – признак соответствия контрольной сумме, CheckSum – полученная контрольная сумма, EtalonCheckSum – эталонная контрольная сумма.

ФБ FileIntegrityControl также имеет выходные параметры: «Running» (отображает статус процесса проверки), «Completed» (сигнализирует об окончании проверки) и «Error» (указывает текст ошибки, если не удалось выполнить проверку).

Регистрация событий безопасности

По умолчанию сообщения типа «Сообщение ИБ» попадают в общий архив сообщений. Однако в ПО MasterSCADA 4D есть возможность формирования отдельной базы данных. Для этих целей в группе «Безопасность» создаётся «Архив сообщений» ИБ (рис. 21).

На рис. 22 показана панель свойств элемента «Архив сообщений».

БД будет иметь по умолчанию имя security_events.db и тип локальной БД – sqlite. Для работы с внешними базами данных PostgreSQL или MSSQL следует выбрать соответствующий тип БД из выпадающего списка и указать параметры подключения (адрес сервера, номер порта, атрибуты пользователя).

Виды событий безопасности

1) Сообщения контроля целостности:

«Ошибка при проверке целостности проекта»

«Ошибка при проверке целостности ПО»

Если проверка целостности будет неудачной, то текст сообщения будет включать в себя код ошибки и список файлов, которые проверку не прошли. Вначале идёт список файлов с отличиями, затем идут пары <код ошибки> <имя файла>.

Коды ошибок:

1 – Файл отсутствует

2 – Ошибка чтения файла

3 – Ошибка в пути к файлу

4 – Несоответствие MD5 сумм

5 – Ошибка дешифрации файла

2) Сообщения по авторизации пользователя.

«Вход в систему» – регистрация успешного запуска сеанса работы.

«Неуспешная попытка входа» – если не пройдена авторизация. Для сообщений данного типа добавляется причина его возникновения:

«Неудачная смена пароля»

«Необходимо сменить пароль»

«Пользователь заблокирован»

«Срок действия пароля истёк»

«Недопустимое время логина»

«Недопустимый адрес логина»

3) Сообщения о блокировке пользователя при превышении количества последовательных неуспешных попыток входа.

Разработчик системы может задать количество последовательных неуспешных попыток входа в свойствах группы «Роли» элемента «Безопасность». Вид формируемого сообщения для такого события:

«Пользователь» + login + «заблокирован по превышению попыток логина».

4) Сообщения об ошибке ключа защиты лицензии.

Система MasterSCADA 4D периодически проверяет доступность ключа в режиме исполнения. Проверка по умолчанию производится раз в 30 минут. В случае если три проверки подряд были неудачными, то работа в режиме исполнения прекращается. При каждой неудачной проверке формируется сообщение, в котором указывается оставшееся время, которое исполнительная система может проработать без ключа.

«Ключ не найден. Проект остановлен».

«Ключ не найден. Проект будет остановлен через %d минут».

Создание гетерогенной среды

Под созданием гетерогенной среды понимается применение различных типов общесистемного, прикладного и специального программного обеспечения в защищённой информационной (автоматизированной) системе.

Среда исполнения MasterSCADA 4D поддерживает большинство распространённых в промышленности операционных систем, таких как Windows, Linux, Эльбрус. В частности, на сайте ГК «Астра» указано, что платформа и клиент визуализации MasterSCADA 4D Client корректно

но работают под управлением ОС Astra Linux. Для применения на производстве и/или в учебном процессе можно использовать рекомендации производителя – компании МПС Софт, оформленные в виде целевого бесплатного курса «Основы Linux для MasterSCADA» [9], описывающего порядок установки Linux, среды исполнения MSRT и клиента визуализации HMI, настройки безопасности, проведение диагностики по стандартным и расширенным лог-файлам.

Защита информации при её передаче по каналам связи

В MasterSCADA 4D предусмотрено использование защищённых протоколов при создании многоуровневой клиент-серверной архитектуры. Для взаимодействия WEB-сервера среды исполнения MasterSCADA 4D и клиентов визуализации/управления предоставляется возможность использовать протокол HTTPS (HyperText Transfer Protocol Secure) – безопасный протокол передачи данных, поддерживается шифрование посредством криптографических протоколов SSL и TLS.

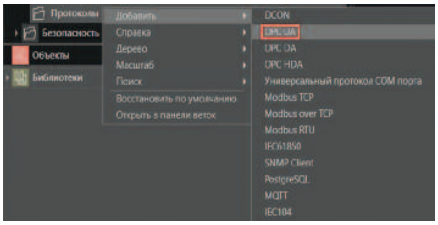


Рис. 23. Создание клиента OPC UA в проекте

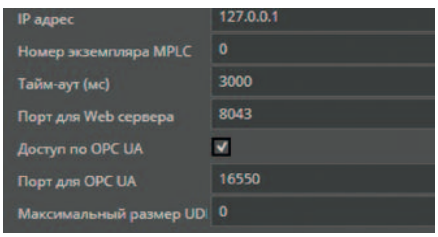


Рис. 24. Настройка параметров узла и сервера OPC UA

Для обмена данными внутри системы промышленной автоматизации может использоваться платформонезависимый стандарт OPC UA. Для того чтобы проект MasterSCADA 4D выступал в роли клиента OPC UA, необходимо в группу узла «Протоколы» добавить соответствующий протокол (рис. 23). Политика безопасности клиента OPC UA позволяет использовать типы шифрования Basic128Rsa15, Basic256, Basic256Sha256.

ПО MasterSCADA 4D может выступать также и как сервер OPC UA (рис. 24), поддерживая режимы чтения и подписки.

Лирическое отступление

Многие тянут с внедрением средств защиты информации на своих объектах, полагаясь на русский «авось» или «не трогай, пока работает». Но в настоящих реалиях незнание или игнорирование информации в этой области может привести к серьёзным последствиям. Как минимум, могут быть сделаны замечания при проведении государственной проверки регулятором (на сайте ФСТЭК России ежегодно обновляются планы проверок компаний по вопросам лицензионного контроля). Как максимум – остановка производства по инцидентам, связанным с атаками злоумышленников. Для понимания современных реалий эксперты рекомендуют периодически анализировать отчёты регуляторов, а также лидеров в области информационной безопасности. Одним из лидеров оперативного информирования по типам, ре-

Таблица 5. Возможности MasterSCADA 4D версии Enterprise для реализации мер защиты

Обозначение меры	Описание меры	Способ реализации в MasterSCADA 4D версии Enterprise
ИАФ.1	Идентификация и аутентификация пользователей и инициируемых ими процессов	Настройки элементов группы «Безопасность» + + библиотечные ФБ
ИАФ.3	Управление идентификаторами	
ИАФ.4	Управление средствами аутентификации	
УПД.1	Управление учётными записями пользователей	
УПД.2	Реализация политик управления доступом	
УПД.4	Разделение полномочий (ролей) пользователей	
УПД.5	Назначение минимально необходимых прав и привилегий	
УПД.6	Ограничение неуспешных попыток доступа в информационную (автоматизированную) систему	Настройки элементов группы «Безопасность»
УПД.9	Ограничение числа параллельных сеансов доступа	
УПД.10	Блокирование сеанса доступа пользователя при неактивности	
АУД.4	Регистрация событий безопасности	Настройки элементов группы «Безопасность» + + настройки локальной БД SQLite или внешних БД PostgreSQL, MSSQL
ОЦЛ.1	Контроль целостности программного обеспечения	Настройки элементов группы «Безопасность» + + библиотечные ФБ
ЗИС.9	Создание гетерогенной среды	Перенос проекта и запуск среды исполнения MSRT на разных ОС: Windows, Linux, Эльбрус
ЗИС.19	Защита информации при её передаче по каналам связи	Настройки проекта для использования защищённых протоколов

комендациям и вариантам защиты от инцидентов является компания «Лаборатория Касперского». На своих вебресурсах она периодически выкладывает обзоры основных международных инцидентов промышленной кибербезопасности. Для примера, за I квартал 2024 года в общей сложности зафиксировано 30 инцидентов, 37% пострадавших сообщили о нарушении операционной деятельности или задержках в отгрузке продукции в результате инцидента. Две трети жертв киберпреступников относятся к сфере производства [10].

Заключение. Перспективы развития учебного стенда

В данной статье мы постарались оотнести возможности пакета MasterSCADA 4D в части функций информационной безопасности с требованиями регулятора, изложенными в документах [5, 6]. Обобщённые результаты этой работы приведены в табл. 5.

Именно этот подход положен авторами в основу концепции стенда. Планируется и дальше развивать и проводить поэтапную модернизацию лаборатории. Опишем некоторые направления.

1) Учебно-методическая деятельность:
   - разработка лабораторных работ по применению мер защиты ИБ;
   - подготовка к защите магистр. диссертации «Комплекс многоуровневой защиты систем промышленной автоматизации»;
   - развитие лаборатории с учётом рекомендаций нового ПРОФСТАНДАРТА МИНТРУДА для специалистов по защите ИБ в автоматизированных системах.
2) Техническое развитие и расширение состава стенда:
   - перенос модулей исполнения MasterSCADA 4D на отечественную ОС Astra Linux. Изучение особенностей использования этой ОС в проектах АСУ ТП;
   - внедрение в состав стенда специализированных наложенных СЗИ (межсетевые экраны, системы обнаружения вторжений);
   - интеграция с современными технологиями машинного обучения и искусственного интеллекта для изучения возможностей более эффективного применения мер защиты.

Отдельно следует отметить, что в составе программной платформы MasterSCADA 4D нет зарубежных компонент, которые могут привести к невозможности его использования в соответствии с требованиями регуляторов и современным российским трендом по технологической независимости. Также производитель программного обеспечения MasterSCADA 4D (Компания ООО «МПС софт») уделяет большое внимание вопросам безопасной разработки программного обеспечения – в настоящее время готовится Руководство по безопасной разработке, испытания по статистическому анализу исходного кода, фаззинг-тестирования. Результаты этой работы будут доступны в ближайшее время. Дополнительную информацию можно запросить через официального дистрибутора этого программного обеспечения – компанию ПРОСОФТ *(info@prosoft.ru)*.

Внимание, важная информация!

20 декабря 2024 года, во время подготовки этой статьи, вышла новая версия ГОСТ Р 56939 («Безопасная разработка ПО»), предъявляющая более жёсткие требования к разработке и контролю ПО, включая процедуры динамического и статического анализа, фаззинг-тестирования кода программного обеспечения российского производства, используемого для обеспечения безопасности значимых объектов критической информационной инфраструктуры РФ (Утверждены приказом ФСТЭК России от 25 декабря 2017 г. № 239).

Компания «МПС софт» в феврале 2025 года провела успешные испытания своего продукта на соответствие требованиям приказа ФСТЭК 239. Специалисты могут ознакомиться с протоколом прохождения испытаний MasterSCADA 4D по отдельному запросу в компанию ПРОСОФТ (info@prosoft.ru).

Литература

1. Банк данных угроз АСУ ТП. URL: https://bduasutp.fstec.ru/ (дата обращения: 10.06.2024).
2. Банк данных угроз АСУ ТП. Объекты воздействия. URL: https://bduasutp.fstec.ru/#/threats/influence-objects (дата обращения: 10.06.2024).
3. Банк данных угроз АСУ ТП. Компоненты. К.4.1.1 Инженер АСУ ТП. URL: https://bduasutp.fstec.ru/#/components-view/3afe8b69-7db5-4b3d-8738-f7078b96c968?from_list=1&query=, (дата обращения: 10.06.2024).
4. *Мухаметшин А.* Как защитить АСУ ТП: экспертиза Innostage // СТА. 2023. № 3.

5. Приказ ФСТЭК России от 25.12.2017 № 239. URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239.
6. Приказ ФСТЭК России от 14.03.2014 № 31. URL https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-14-marta-2014-g-n-31.
7. Банк данных угроз АСУ ТП. Меры защиты. URL: https://bduasutp.fstec.ru/#/bdu/protection-measures (дата обращения: 10.06.2024).
8. MasterSCADA 4D справочная система, web-версия. URL: https://support.mps-soft.ru/Help-web/index.html.
9. Курс 3519 «Основы Linux для MasterSCAD». URL: https://lms.iek.group/content/info/7275.
10. Краткий обзор основных инцидентов промышленной кибербезопасности за первый квартал 2024 года. URL: https://ics-cert.kaspersky.ru/publications/reports/2024/06/03/q1-2024-a-brief-overview-of-the-main-incidents-in-industrial-cybersecurity/.
11. Приказ министерства труда и социальной защиты Российской Федерации от 14.09.2022 № 525н «Об утверждении профессионального стандарта “Специалист по защите информации в автоматизированных системах”». URL: https://docs.cntd.ru/document/352000921#6560IO.

НОВОСТИ реклама НОВОСТИ реклама

Новая модель встраиваемого компьютера AdvantiX ER-8200

Компания Advantix представила новую модель встраиваемого компьютера AdvantiX ER-8200, предназначенную для выполнения ресурсоёмких приложений и работы в ответственных системах управления, например, в области энергетики, на производстве, в транспортной сфере: управление движением транспорта, грузоперевозками, организация обслуживания пассажиров и др.

Высокопроизводительная новинка ER-8200 реализована на базе новейших процессоров Intel 11-го поколения: Intel Core i5-1135G7, Quad-core, до 4,20 ГГц или Intel Core i7-1165G7, Quad-core, до 4,70 ГГц.

Мощные графические возможности AdvantiX ER-8200 обеспечиваются интегрированной графической системой Intel Iris Xe G7 (80/96 блоков EU) с парой выходов HDMI на борту.

Основные преимущества AdvantiX ER-8200

- Реализована на базе новейших процессоров Intel 11-го поколения: Intel Core i5-1135G7 или Intel Core i7-1165G7.
- Гибкие возможности выбора конфигурации: RAM – до 64 Гбайт DDR4, M.2 SSD, установка слотов расширения: 1× M.2 Key-M Slot; 1× M.2 Key-E Slot; 1× Mini PCI-E Slot. ●

Новый Президент Санкт-Петербургской Российской секции ISA

1 января 2025 года в должность Президента Санкт-Петербургской Российской секции ISA вступил Солёный Сергей Валентинович – проректор по образовательным технологиям и инновационной деятельности ГУАП, кандидат технических наук, доцент. ●