УДК 004.056.5 Вестник УрФО № 2(48) / 2023, с. 42–48

Заид Алкилани М.О., Машкина И. В.

DOI: 10.14529/secur230203

ПОЛИТИКА КОНТРОЛЯ ДОСТУПА В АВТОМАТИЗИРОВАННОЙ СИСТЕМЕ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМ ПРОЦЕССОМ (АСУ ТП)

Цель работы: В статье основное внимание уделяется использованию модели управления доступом на основе ролей (Role-Based Based Access Control, RBAC) для разработки политики контроля доступа в автоматизированной системе управления технологическим процессом(АСУТП). Представлены информационные активы корпоративной системы, необходимые для работы промышленной сети. По итогам проделанной работы определены роли пользователей и административные роли. Построена иерархия ролей пользователей с установлением ограничений, для обеспечения безопасности информационной системы. разработана матрица разграничения доступа к сети.

Ключевые слова: *автоматизированная система управления технологическим процессом АСУТП, информационные объекты, информационные субъекты, разграничение доступа, управление учетными записями и правами пользователей, иерархия ролей пользователей.*

Zaid Alkilani M.O., Mashkina I.V.

ACCESS CONTROL POLICY IN INDUSTRIAL CONTROL SYSTEM (ICS)

Purpose of work: This paper focuses on recommending the use of a Role-Based Access Control (RBAC) model for developing access control policies in an industrial control system (ICS). The form displays the information assets of the company system required to operate the industrial network. Based on the results of the work performed, user roles and administrative roles are determined. A hierarchy of user roles has been created with restrictions in place to ensure the security of the information system. Differentiation Matrix was developed in Access Network.

Keywords: *Industrial control system ICS, information objects, information subjects, access control, user account and rights management, user role hierarchy.*

Введение

Сфера применения информационных систем постоянно расширяется. АСУ ТП - это общий термин, используемый для описания интеграции аппаратного и программного обеспечения с сетевым подключением для поддержки критически важной инфраструктуры. Технологии АСУ ТП включают в том числе: диспетчерское управление и сбор данных (Supervisory control and data acquisition, SCADA), распределенные системы управления (РСУ, DCS), программируемые логические контроллеры (ПЛК, PLCs), контроллеры и удаленные терминалы (remote terminal units, RTU), серверы управления, интеллектуальные электронные устройства (ИЭУ) и датчики. АСУ ТП в настоящее время используют открытые архитектуры, они часто подключаются к внешним системам, таким как офисные системы. Сегодня устройства АСУ ТП и протоколы, используются практически во всех отраслях промышленности, таких как производство, транспорт, энергетика и т. д. [1, 2].

Из-за природы открытых сред безопасность систем SCADA по своей сути является сложной проблемой: компьютерный инцидент в системах SCADA это один из критических инцидентов, которые оказывают значительное влияние на безопасность производства, персонала, экологии окружающей среды [3]. Кроме того, управление системами SCADA является важнейшей задачей, требующей от системных администраторов управления большим количеством объектов и функций, связанных с распределенными критически важными инфраструктурами. Требования, установленные в приказе ФСТЭК России № 31 [4], направлены на обеспечение функционирования АСУ ТП в штатном режиме, следовательно, это также приводит к сложности политик безопасности и создает потребность в поиске систематического способа формулирования [5].

Как правило, политики безопасности разрабатываются для защиты критически важных активов в системах SCADA вместе с соответствующими механизмами безопасности. Есть много элементов, которые являются частью политики безопасности предприятия. В нескольких статьях [6, 7] представлены структуры высокого уровня для управления политиками безопасности SCADA. Однако ни одна из этих работ не предоставила систематического способа сформулировать все элементы, необходимые для определения и обеспечения соблюдения политик безопасности в АСУ ТП. Многоуровневая архитектура АСУ ТП с учетом возможных вариантов построения приведена в работе [5].

Контроль доступа к данным — это метод, используемый для регулирования доступа сотрудников к информационным ресурсам организации. Он включает в себя использование принципа наименьших привилегий, общий подход для всех моделей как раз и состоит в разделении множества сущностей, составляющих систему, на множества субъектов и объектов. В общем строим ролевую модель управления доступом RBAC.

В этой статье предлагается использовать метод RBAC, предложенный в [9 10], чтобы решить проблемы управления доступом в АСУ ТП, для этого необходимо создать функциональную модель каждого подразделения и указать должности, провести аудит ИТ-систем и расставить их по приоритетам, нужно создать бизнес-ориентированное описание прав пользователей [8].

RBAC обеспечивает большую гибкость в том, как администраторы назначают разрешения и роли пользователям. Пользователи имеют доступ к разрешениям, связанным с ролями, и пользователи становятся членами соответствующих ролей. Пользователям можно назначать роли на основе их должностных инструкций и функций, и их можно легко переназначать из той или иной роли или полностью удалять из системы без изменения базовой структуры управления доступом. Ролям могут быть предоставлены новые разрешения, когда это необходимо, и разрешения могут быть удалены из роли по мере необходимости. В этой статье получим компоненты управления доступом, включая пользователей (субъект) роли, объекты, операции и разрешения для таких компонентов, АСУ ТП как SCADA и другие. Пользователь — это человек или автономный агент, роль — это должностная функция или должность в организации с некоторой связанной семантикой, касающейся полномочий и ответственности, возложенных на члена роли, а разрешение — это одобрение определенного режима доступа к одному или нескольким объ-

ектам в системе или некоторых привилегий для выполнения определенных действий. Объекты состоят из наборов ресурсов, которые содержат или получают информацию.

Как правило, пользователь имеет доступ к объекту на основе назначенной ему роли, которая определяется на основе его функции в организации. Объект касается роли пользователя. Полномочия определяются на основе должностных полномочий и обязанностей в рамках должностной функции. Операции над объектом вызываются на основе разрешений. Роли организованы в частичном порядке, Каждый сеанс связывает одного пользователя со многими ролями. Идея состоит в том, что пользователь устанавливает сеанс и активирует некоторое подмножество ролей, членом которых он является (прямо или косвенно посредством иерархии ролей) [11–14].

Результаты исследований

Чтобы определить требования к контролю доступа в АСУ ТП, необходимо собрать достаточную информацию о системах АСУ ТП и определить все компоненты, имеющие право доступа. Политика безопасности контроля доступа начинается с определения критических и важных ресурсов, затем определения того, кто может получить доступ к этим ресурсам, и точного знания, какой доступ предоставляется. Необходимо определить роли в организации АСУ ТП и подробно описать тип доступа к критически важным ресурсам, действиям и операциям. Модель управления доступом описывает объекты как ресурсы (например, аппаратное обеспечение, датчик, робот, таблицу базы данных и т. д.), а субъекты — как сущности, инициирующие запрос на доступ.

В таблицах ниже представлены субъекты и объекты системы АСУ ТП.Для формального описания частной политики безопасности — политики разграничения доступа к информационным объектам АСУ ТП используем математическую ролевую модель доступа.

Понятие «иерархия управления» представляет собой порядок подчинения элементов одного уровня элементами другого в пределах системы управления, который используется в базах данных и в системах компьютерной безопасности. Данное понятие тесно связанно с понятием «система управления». В системах управления существуют понятия «элемент системы», «подсистема», «часть системы», являющиеся управляющими и управляемыми, которые имеют характеристики

Таблица 1

Набор информационных объектов и субъектов доступа

Множество объектов доступа	
Наименование	***Обозн***
SCADA (приложение)	o1
Человеко-машинный интерфейс HMI	o2
Программное обеспечение OPC сервера	o3
MES, ERP (приложения)	o4
База архивных данных	o5
База оперативных данных	o6
Планы Планы технологических процессов,Техническое задание (операционные картины, маршруты, этапы операции)	o7
Настройки ПЛК (инструкции)	o8
Алгоритм управления ПЛК	o9
Управляющие сигналы контроллерам	o10
Данные о сигналах с измерительных датчиков	o11
Сведения о протоколах связи (ModbusRTU/TCб, DNP3.0, PROFIBUS, IEC …)	o12
Данные о настройках и обслуживании оборудования	o13
Данные о сигналах тревоги	o14
Данные о системе тревожной сигнализации (изменение точек тревоги, установка предельного значения)	o15
Сведения о сети (таблицы коммутации и маршрутизации)	o16
Текущие настройки (конфигурации)	o17
Подсистема генерациографических и текстовых отчетов	o18

Окончание таблицы 1

Множество субъектов доступа	
Наименование	***Обозн***
Руководитель	PY
ERP менеджер	ER1
MES менеджер	MES1
Начальник (Производства)	N1
Scada инженер	SE
Диспетчер	D
Специалист по вычислительной технике	CT
Технолог	TE
Оператор	OP
Инженер по обслуживанию технологического оборудования	ES
Специалист по обслуживанию измерительного оборудования	TM
Администратор безопасности	SA
Администратор сети	NA
Администратор	A
Сотрудник	S

для управляющих и исполнительных элементов. Иерархия ролей является организационным термином, и выделяет подсистемы управления, полагаясь на признак функциональности. Иерархией ролей в модели RBAC называется заданное на множестве ролей R отношение частичного порядка «≤», при котором выполняется условие: для $u \in U$, если r_i, $r_j \in R$, $r_j \in UA(u)$ и $r_i \le r_j$, то $r_i \in UA(u)$. Таким образом, наряду с ролью r_j пользователь должен быть авторизован на все роли, в иерархии ее меньшие. Аналогичным образом строится иерархия административных ролей на множестве административных ролей AR. Перенимая все упомянутое, они не теряют атрибутов своих прошлых ролей. Они наследуют дополнительные атрибуты, обязанности и связанные с ними переменные роли, которые они берут на себя, не теряя при этом никаких атрибутов своих прежних ролей. Взяв во внимание данные исследования, подготовлена иерархическая структура ролей в системе управления технологическим процессом (рис. 1).

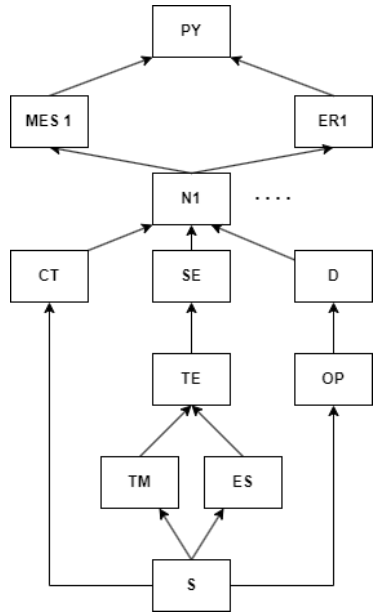

Рис. 1. иерархическая структура ролей в АСУ ТП (PYРуководитель, ER1ER1 менеджер, MES1 менеджер: MES, N1Начальник, SEScada инженер, DДиспетчер, CTСпециалист по вычислительной технике, TE Технолог, OPОператор, ESИнженер по обслуживанию технологического оборудования, TMСпециалист по обслуживанию измерительного оборудования, S Сотрудник)

Строки соответствуют субъектам доступа, столбцы — объектам доступа, а разрешенные операции (права) субъекта на объект записывают в ячейки. В матрице используются следующие обозначения: w – «write, записать», r – «read, прочитать», e – «execute, выполнить» c – «create, создавать» and d – «delete, удалить». Политика разграничения доступа в АСУТП разработана на основе таблицы 1 и иерархии ролей, представленной на рисунке 1 в формате прямоугольной матрицы (таб. 2).

Таблица 2

Матрица разграничения доступа в АСУТП

Обозн	o1	o2	o3	o4	o5	o6	o7	o8	o9
PY	*rwecd*	*wec*	*rwecd*	*re*	*rcd*	*rwcd*	*rwecd*	*rwecd*	*rwecd*
ER1	*rwecd*	*wec*	*rwecd*	*re*	*rcd*	*rwcd*	*rcd*	*rwecd*	*rwecd*
MES1	*rwecd*	*wec*	*rwecd*	*re*	*rcd*	*rwcd*	*rwecd*	*rwecd*	*rwecd*
N1	*rwecd*	*wec*	*rwecd*	*re*	*rcd*	*rcd*	*rcd*	*rwecd*	*rwecd*
CT	*rcd*	*wec*	*rcd*	*e*	*rcd*	*rcd*	*rcd*	*rdc*	*rdc*
D	*r*	*e*	*r*	*r*	*r*	*r*	*r*	*r*	
OP	*r*	*e*	*r*	*r*	*r*	*r*	*r*	*r*	
SE	*rwe*	*e*	*rwc*	*re*	*r*	*rw*	*r*	*rwe*	*rwe*
TE	*r*	*e*	*r*	*r*	*r*		*r*	*re*	*re*
TM				*r*	*r*		*r*		
ES				*r*	*r*		*r*		
S				*r*	*r*		*r*		

Окончание таблицы 2

Матрица разграничения доступа в АСУТП

Обозн	o10	o11	o12	o13	o14	o15	o16	o17	o18
PY	*rwecd*	*rwe*	*rwe*	*rwe*	*r*	*rwde*	*rwe*	*rwe*	*rwecd*
ER1	*rwecd*	*rwe*	*rwe*	*rwe*	*r*	*rwde*	*rwe*	*rw*	*rwecd*
MES1	*rwecd*	*rwe*	*rwe*	*rwe*	*r*	*rwde*	*rwe*	*rwe*	*rcd*
N1	*rwecd*	*rwe*	*rwe*	*rwe*	*r*	*rwde*	*rwe*	*rw*	*rcd*
CT	*rcd*	*rwe*	*r*	*r*	*r*	*r*	*r*	*rw*	*rcd*
D	*r*	*r*		*r*	*r*	*re*		*r*	*r*
OP	*r*	*r*		*r*	*r*	*r*		*r*	*r*
SE	*rwe*	*rwe*	*rwe*	*rwe*	*r*	*r*	*rwe*	*rw*	*r*
TE	*rwe*	*rwe*	*rwe*	*rwe*	*r*	*r*	*rwe*	*rw*	*r*
TM	*re*	*re*		*e*	*r*	*r*	*r*	*rw*	*r*
ES	*rw*	*rw*		*rw*	*r*	*r*	*r*	*r*	*r*
S							*r*		*r*

Заключение

В данной работе рассмотрены политики управления доступом к данным, разработана методика формализации правил взаимодействия информационных субъектов и объектов в АСУ ТП с использованием математической модели RBAC, основанной на группировании прав доступа субъектов АСУ ТП к объектам с учетом специфики их применения. Предлагаемая методика отличается определением множества объектов доступа, специфичных для АСУ ТП, введением подробной иерархической структуры субъектов доступа.

Литература

1. Мотаз Аль Медирес, Мохаммед Аль Майа, Кибербезопасность в системе промышленного управления (АСУТП), Международная конференция по информационным технологиям (ICIT), 2021 г., IEEE DOI: 10.1109/ICIT52682.2021.9491741, С. 640–648.

2. Закария Дриас, Ахмед Серручни, Оливье Фогель, Анализ кибербезопасности для промышленных систем управления, август 2015 г., вы можете найти на https://www.researchgate.net.

3. Джо Вайс, Книга: Промышленная система управления (ICS) Кибербезопасность для систем водоснабжения и водоотведения, октябрь 2014 г., DOI: 10.1007/978-3-319-01092-2_3.

4. Приказ ФСТЭК России от 14 марта 2014 г. N 31 "Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды".

5. Ирина Машкина, Ильдар Гарипов, Разработка модели объекта защиты – Промышленной системы управления с использованием системного анализа. Опубликовано в: Международная российская конференция по автоматизации 2018 года (RusAutoCon). Дата проведения конференции: 9-16 сентября 2018 года. Дата добавления в IEEE Xplore: 22 октября 2018 года. Информация об ISBN: Электронный ISBN: 978-1-5386-4938-1, печать по запросу(PoD) ISBN: 978-1-5386-4939-8, регистрационный номер журнала: 18168367. DOI: 10.1109/RUSAUTOCON.2018.8501733. Издатель: IEEE. Место проведения конференции: Сочи, Россия. Скопус https://ieeexplore.ieee.org/document/8501733.

6. Мехди Асгархани и Елена Ситникова, Журнал информационных войн, Разработка стратегической основы для управления безопасностью в системах SCADA, Vol. 13, № 4 (2014), С. 70–84.

7. Донг-Джу Кан, Юнг-Джу Ли, Сеог-Джу Ким, Йонг-Хван Мун, IFAC Proceeding Volumes, Проектирование системы безопасности для сети SCADA Power System, том 42, выпуск 9, 2009 г., С. 227–232.

8. Алессандро Риччи, Мирко Вироли, Андреа Омичини, Управление доступом на основе ролей в MAS с использованием контекстов координации агентов, доступно в Интернете на сайте researchgate с 16 мая 2004 г. по ссылке https://t.ly/TU_T3.

9. ГОСТ Р 59453.1-2021, Защита информации. Формальная модель управления доступом. Часть 1. Общие положения, 01.06.2021, по ссылке https://protect.gost.ru/document1.aspx?control=31&baseC=6&page=2&month=5&year=2021&search=&id=240521.

10. Корт С.С. Теоретические основы защиты информации: учебное пособие. –М.: Гелиос АРВ,2004. –240 с., ил.

11. Ишан Асафл, Мухаммад Асад, Шафик Ахмед, Вакас Рашид, Тарик Башир, Международная конференция по системам и технологиям с открытым исходным кодом (iCOSST), Вопросы архитектуры управления доступом на основе ролей в крупных организациях, 3, 2014 г.

Грегори Сондерс, Майкл Хитченс и Виджай Варадхараджан, журнал researchgate, управление доступом на основе ролей и матрица управления доступом. Школа информационных технологий Сиднейского университета, Австралия, 2014 г.

12. Мауро Онори, Антонио Маффеи, researchgate портал, «Применение модели управления доступом на основе атрибутов к промышленным системам управления», статья в Международном журнале компьютерных сетей и информационной безопасности, февраль 2017 г.

13. Мунир Маджалавиех, Франческо Паризи Пресикче, Рави Сандху, Модель RBAC для SCADA, Инновационные алгоритмы и методы автоматизации, промышленной электроники и телекоммуникаций, С. 329–335, 2007 г.

Reference

1. Motaz Al' Medires, Mokhammed Al' Maya, Kiberbezopasnost' v sisteme promyshlennogo upravleniya (ASUTP), Mezhdunarodnaya konferentsiya po informatsionnym tekhnologiyam (ICIT), 2021 g., IEEE DOI: 10.1109/ICIT52682.2021.9491741, S. 640–648.

2. Zakariya Drias, Akhmed Serruchni, Oliv'ye Fogel', Analiz kiberbezopasnosti dlya promyshlennykh sistem upravleniya, avgust 2015 g., vy mozhete nayti na https://www.researchgate.net.

3. Dzho Vays, Kniga: Promyshlennaya sistema upravleniya (ICS) Kiberbezopasnost' dlya sistem vodosnabzheniya i vodootvedeniya, oktyabr' 2014 g., DOI: 10.1007/978-3-319-01092-2_3.

4. Prikaz FSTEK Rossii ot 14 marta 2014 g. N 31 (ob utverzhdenii trebovaniy k obespecheniyu zashchity informatsii v avtomatizirovannykh sistemakh upravleniya proizvodstvennymi i tekhnologicheskimi protsessami na kriticheski vazhnykh ob"yektakh, potentsial'no opasnykh ob"yektakh, a takzhe ob"yektakh, predstavlyayushchikh povyshennuyu opasnost' dlya zhizni i zdorov'ya lyudey i dlya okruzhayushchey prirodnoy sredy).

5. Irina Mashkina; Il'dar Garipov. Razrabotka modeli obekta zashchity – Promyshlennoj sistemy upravleniya s ispol'zovaniem sistemnogo analiza. Opublikovano v: Mezhdunarodnaya rossijskaya konferenciya po avtomatizacii 2018 goda (RusAutoCon). Data provedeniya konferencii: 9-16 sentyabrya 2018 goda. Data dobavleniya v IEEE Xplore: 22 oktyabrya 2018 goda. Informaciya ob ISBN: Elektronnyj ISBN: 978-1-5386-4938-1, pechat' po zaprosu(PoD) ISBN: 978-1-5386-4939-8, registracionnyj nomer zhurnala:

18168367. DOI: 10.1109/RUSAUTOCON.2018.8501733. Izdatel': IEEE. Mesto provedeniya konferencii:Sochi, Rossiya. Skopus https://ieeexplore.ieee.org/document/8501733.

6. Mekhdi Asgarkhani i Yelena Sitnikova, Zhurnal informatsionnykh voyn, Razrabotka strategicheskoy osnovy dlya upravleniya bezopasnost'yu v sistemakh SCADA, Vol. 13, № 4 (2014), S. 70–84.

7. Dong-Dzhu Kan, Yung-Dzhu Li, Seog-Dzhu Kim, Yong-Khvan Mun, IFAC Proceeding Volumes, Proyektirovaniye sistemy bezopasnosti dlya seti SCADA Power System, tom 42, vypusk 9, 2009 g., S. 227–232.

8. Alessandro Richchi, Mirko Viroli, Andrea Omichini, Upravleniye dostupom na osnove roley v MAS s ispol'zovaniyem kontekstov koordinatsii agentov, dostupno v Internete na sayte researchgate s 16 maya 2004 g. po ssylke https://t.ly/TU_T3.

9. GOST R 59453.1-2021, Zashchita informacii. Formal'naya model' upravleniya dostupom. Chast' 1. Obshchie polozheniya, 01.06.2021, po ssylke https://protect.gost.ru/document1.aspx?control=31&baseC=6&page=2&month=5&year=2021&search=&id=240521.

10. Kort S.S. Teoreticheskie osnovy zashchity informacii: Uchebnoe posobie. –M.: Gelios ARV,2004. – 240 s., il.

11. ishan Asafl, Mukhammad Asad, Shafik Akhmed, Vakas Rashid, Tarik Bashir, Mezhdunarodnaya konferentsiya po sistemam i tekhnologiyam s otkrytym iskhodnym kodom (iCOSST), Voprosy arkhitektury upravleniya dostupom na osnove roley v krupnykh organizatsiyakh, Z, 2014 g.

12. Gregori Sonders, Maykl Khitchens i Vidzhay Varadkharadzhan, zhurnal researchgate, upravleniye dostupom na osnove roley i matritsa upravleniya dostupom. Shkola informatsionnykh tekhnologiy Sidneyskogo universiteta, Avstraliya, 2014 g.

13. Mauro Onori, Antonio Maffei, researchgate portal, «Primeneniye modeli upravleniya dostupom na osnove atributov k promyshlennym sistemam upravleniya», stat'ya v Mezhdunarodnom zhurnale komp'yuternykh setey i informatsionnoy bezopasnosti, fevral' 2017 g.

14. Munir Madzhdalaviyekh, Franchesko Parizi Presikche, Ravi Sandkhu, Model' RBAC dlya SCADA, Innovatsionnyye algoritmy i metody avtomatizatsii, promyshlennoy elektroniki i telekommunikatsiy, S. 329–335, 2007 g.

МУХАННАД Осама Заид Алкилани, аспирант 3 курса по специальности «Информационная безопасность», Уфимский государственный авиационный технический университет. 450008, Россия, Республика Башкортостан, г. Уфа, ул. К. Маркса, 12. E-mail: muhannad.killani@gmail.com

МАШКИНА Ирина Владимировна, доктор технических наук, профессор, Факультет Информатики и Робототехники. Уфимский государственный авиационный технический университет. 450008, Россия, Республика Башкортостан, г. Уфа, ул. К. Маркса, 12. E-mail: profmashkina@mail.ru

MUHANNAD Osama Zaid Alkilani, 3rd year postgraduate student in the specialty "Information Security", Ufa State Aviation Technical University. 450008, Russia, Republic of Bashkortostan, Ufa, st. K. Marx, 12. E-mail: muhannad.killani@gmail.com

MASHKINA Irina Vladimirovna, Doctor of Technical Sciences, Professor, Faculty of Informatics and Robotics. Ufa State Aviation Technical University. 450008, Russia, Republic of Bashkortostan, Ufa, st. K. Marx, 12. E-mail: profmashkina@mail.ru