УДК 004.056.5

ПОДХОД К РАЗРАБОТКЕ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АСУ ТП ДЛЯ АВТОМАТИЗАЦИИ ПРОЦЕССОВ УПРАВЛЕНИЯ ДОСТУПОМ

И.И. ЗАБИРОВ [1], И.В. МАШКИНА[2]

[1] Ildar.zabirov.lord@mail.ru, [2] profmashkina@mail.ru

ФГБОУ ВО «Уфимский университет науки и технологий» (УУНиТ)

Аннотация. Предложено для снижения нагрузки на администратора безопасности и обеспечения более высокого уровня информационной безопасности использовать в АСУ ТП *IdM/IAM* системы, позволяющие автоматизировать процессы управления правами доступа. В статье приводится перечень информационных сущностей: информационных объектов и субъектов доступа, специфичных для промышленной сети. Разработана иерархическая схема ролей пользователей.

Ключевые слова: информационные объекты; информационные субъекты; разграничение доступа; управление учетными записями и правами пользователей; иерархия ролей пользователей.

ВВЕДЕНИЕ

Информационная безопасность (ИБ) автоматизированных систем управления технологическими процессами (АСУ ТП), которые относятся к значимым объектам критической информационной инфраструктуры (КИИ), регламентируется требованиями, приведенными в приказах ФСТЭК №235 и №239 [1,2]. Требования, установленные в приказе ФСТЭК №31 [3], направлены на обеспечение функционирования АСУ ТП в штатном режиме, при котором обеспечивается соблюдение проектных пределов значений параметров выполнения целевых функций в условиях воздействия угроз нарушения безопасности информации на промышленных объектах, объектах топливно-энергетического комплекса, атомной энергетики, транспортной инфраструктуры, гидротехнический сооружений. Многоуровневая архитектура АСУ ТП с учетом возможных вариантов построения приведена в работе [4]. В работе [5] приведены результаты анализа угроз нарушения ИБ целевых объектов АСУ ТП, реализуемых потенциально возможным злоумышленником или нарушителем.

При создании или модернизации АСУ ТП важная часть работ связана с обеспечением защиты информации, обрабатываемой в системе, путем использования совокупности организационных, технических мер защиты, разработки политики безопасности. Система защиты информации (СЗИ) в АСУ ТП разрабатывается и внедряется на основе сформированных заказчиком требований к защите информации в соответствии с установленным классом автоматизированной системы. Совокупность мер защиты, которые требуется реализовать в СЗИ АСУ ТП соответствующих классов защищенности, приведена в приложении к приказу ФСТЭК №31, она включает в себя 17 групповых мер. Важнейшей из групповых мер является «Управление доступом». В состав этой группы мер входят: разработка политики управления доступом, управление учетными записями пользователей, реализация политики управления доступом, разделение полномочий (ролей) пользователей, назначение минимальных необходимых прав, управление атрибутами безопасности, контроль доступа из внешних информационных (автоматизированных) систем и др.

Рассмотрим, как и с помощью каких средств защиты реализуются данные требования к защите АСУ ТП. Для реализации данной групповой меры разработаны системы *Identity and Acccess Management (IdM/IAM)*, которые включают в себя комплекс системных программных средств для управления учетными записями, контроля и управления доступом пользователей с целью повышения эффективности защиты.

Чем более важной и ценной является обрабатываемая в АСУ ТП информация, тем более сложными должны быть механизмы контроля доступа. Управление учетными записями пользователей основывается на разработанной политике управления доступом, которая является частной политикой безопасности и создается в рамках административной политики. Она предписывает, кому из пользователей и при каких условиях могут предоставляться информационно-вычислительные ресурсы. Механизмы контроля доступа должны быть настроены на реализацию этой частной политики безопасности. Используются известные модели разграничения доступа, например, мандатская, ролевая. Правила доступа групп предусмотрены в *Windows Network Systems, Kerberos, RADIUS, TACACS*, списки доступа используются в маршрутизаторах.

В настоящее время на рынке представлено большое число *IdM/IAM*, некоторые из них:

- *Ankey IDM* (газинформ сервис) программный продукт для централизованного управления учетными записями пользователей и их полномочиями в корпоративных сетях [6];
- *IBM Security Access Manager for Enterprise Sign-On (IBM)* автоматизация доступа пользователей ко всем корпоративным приложениям, с использованием политик и профилей доступа [7];
- *Active Roles (One Identity)* – управление учетными записями и идентификационными данными пользователей и групп на основе ролевой модели [8];
- *Avanpost IDM* (Аванпост) – это отечественная IDM – система для централизованного управления учетными записями и правами доступа пользователей к корпоративным ресурсам [9].
- *Oracle Identity Manager (Oracle)* – это система для управления учетными записями и привилегиями пользователей информационных ресурсов предприятия [10].
- *IDM*. Управление учетными данными» на платформе 1С Предприятия – является универсальной системой для автоматизации процессов централизованного управления учетными записями и правами доступа пользователей в информационных системах [11].

Использование *IdM/IAM* систем позволяет обеспечить централизованное управление учетными записями, паролями и правами на доступ к информационным объектам. Посредством коннекторов обеспечивается подключение системы к компонентам инфраструктуры АСУ ТП, на которых обрабатываются информационные ресурсы компании. Далее процесс управления учетными записями и правами производится через *IdM/IAM* систему.

Как правило, схема реализуется с помощью следующих компонентов (рис. 1):

- сервер *IdM/IAM*;
- база данных *IdM/IAM*;
- коннекторы (для подключения оконечным компонентам инфраструктуры);
- консоль администратора;
- консоль различных групп пользователей.

Рис. 1. Схема *IdM/IAM*

Система управления учетными записями делится на подсистемы для реализации следующих функций:

- Создание, изменение, удаление учетных записей, согласование и назначение прав доступа к информационным объектам - *Identity manager (IDM)*;
- Аутентификация, авторизация, аудит - шлюз безопасности при доступе к приложениям *Access Manager (AM)*;
- Регистрация, прозрачный доступ ко всем приложениям и управление паролями - *Enterprize Single Sign-On (ESSO).*

Для обеспечения функционирования системы управления учетными записями и доступом в промышленной сети необходимо разработать иерархию ролей пользователей АСУ ТП, на ее основе – матрицу разграничения доступа.

В систему управления учетными записями необходимо внести информацию о сотрудниках АСУ ТП, назначить права доступа каждого сотрудника в соответствии с его должностными обязанностями. Необходима интеграция *IdM/IAM* с кадровой системой.

Исходной информацией для разработки иерархии ролей и матрицы разграничения доступа служат доверенные источники: приложения отдела кадров компании. Это сведения о приеме, увольнении сотрудников, отпуске и т. д. В *IdM/IAM* реализован функционал управления правами доступа в компании (создание, изменение прав доступа, удаление учетных записей, блокирование), а также функционал, реализующий возможность организовать процесс по запросу изменений в учетных данных сотрудников.

Результаты исследований, существующих в АСУ ТП должностей и информационных объектов представлены далее в табл. 1.

Таблица 1

Перечень субъектов и объектов доступа в АСУ ТП

Наименование	***Обозначение***
Множество объектов доступа	
Приложение - программный пакет *SCADA*	*O1*
База архивных данных	*O2*
База оперативных данных	*O3*
Приложение - программное обеспечение *OPC*	*O4*
Алгоритмы управления для *PLC*	*O5*
Программное обеспечение *PLC*	*O6*
Техническое задание	*O7*
Технологические системы АСУ: операционные карты, маршруты, этапы операций	*O8*
Контроль над технологическими процессами производства	*O9*
Графики планов технического обслуживания, ремонтов	*O10*
Аналитические данные(отчеты) критически важных показателей	*O11*
Приложения *MES, ERP*	*O12*
HMI	*O13*
Данные для управления системой автоматизации(Управляющие программы производства 1)	*O14*
Данные для управления системой автоматизации(Управляющие программы производства 2)	*O15*
Данные с контрольно-измерительного оборудования производства 1	*O16*
Данные с контрольно-измерительного оборудования производства 2	*O17*
Данные о сети(таблицы маршрутизации и коммутации)	*O18*
Множество ролей	
Сотрудник	*S*
Инженер по обслуживанию технологического оборудования	*IT*
Специалист по вычислительной технике производства 1	*P1*
Инженер по качеству 1	*IK1*
Технолог 1	*T1*
Оператор 1	*OP1*
Инженер АСУ 1	*IA1*
Начальник производства 1	*N1*
Специалист по вычислительной технике производства 2	*VT2*
Инженер по качеству 2	*IK2*
Технолог 2	*T2*
Оператор 2	*OP2*
Инженер АСУ 2	*IA2*
Начальник производства 2	*N2*
Директор	*D*

Управление доступом с использованием ролевой модели повышает уровень ИБ компании, так как доступ становится более прозрачным, управляемым и контролируемым. Результаты исследования должностных обязанностей и множество ролей пользователей АСУ ТП представлены в виде иерархии ролей на рис. 2.

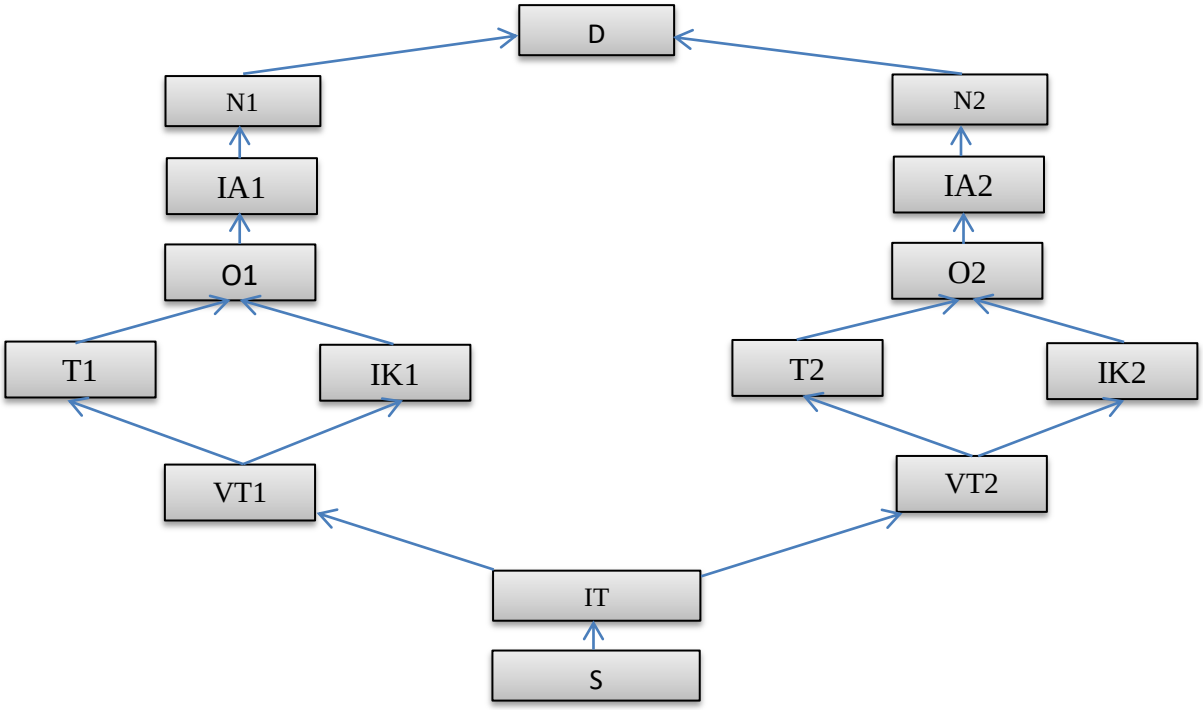

Рис. 2. Иерархическая схема ролей пользователей АСУ ТП

На основе сформированных списков информационных субъектов и объектов доступа в АСУ ТП и разработанной иерархии ролей для настройки *IdM/IAM* системы заполняется матрица разграничения доступа, в которой по вертикали вносятся роли пользователей в соответствии с иерархической схемой, по горизонтали – информационные объекты доступа, на пересечении – возможные права: чтение, запись, выполнение программы, удаление, создание.

ЗАКЛЮЧЕНИЕ

В данной статье проведен анализ комплекса системных программных средств для управления учетными записями, контроля и управления доступом пользователей, с целью повышения эффективности защиты. Рассмотрен не только состав модулей этой системы, но и функционал, особенности работы *IdM/IAM* системы и функции подсистем.

В рамках разработки частной политики ИБ – политики управления доступом предложена схема информационных сущностей ролевой модели разграничения доступа в АСУ ТП.

Разработана иерархическая схема ролей пользователей промышленной сети предприятия.

СПИСОК ЛИТЕРАТУРЫ

1. Приказ ФСТЭК России от 14.03.2014 N 31 (ред. от 15.03.2021) "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".

2. Приказ ФСТЭК России от 21.12.2017 N 235 (ред. от 27.03.2019) "Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования".

3. Приказ ФСТЭК России от 25.12.2017 N 239 (ред. от 20.02.2020) "Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации".

4. Mashkina I., Garipov I., Development of Protection Object Model – Industrial Control System Using System Analysis. Published in 2018 International Russia Automation Conference (RUSAutoCon). Date of Conference: 9-16 Sept. 2018. Date Added to IEEE Xplore:

22 october 2018. ISBN Information: Electronic Number: 18168367. DOI: 10.1109/RUSAUTOCON.2018.8501733. Publisher: IEEE. Conference Location: Sochi, Russia. Scopus https://ieeexplore.ieee.org/document/8501733.

5. Машкина И., Гарипов И., РАЗРАБОТКА EPC - моделей угроз нарушения информационной безопасности автоматизированной системы управления технологическими процессами. Журнал. Безопасность информационных технологий. Том 26, №4(2019). ВАК доступно в электронном виде по ссылке: https://bit.mephi.ru/index.php/bit/article/view/1172.

6. Ankey IDM URL : https://www.gaz-is.ru/produkty/upravlenie-ib/ankey-idm.html.

7. IBM Security Access Manager for Enterprise Sign-On. URL: https://www.oracle.com/middleware/technologies/enterprise-single-sign-on.html.

8. Active Roles. URL: https://www.oneidentity.com/products/active-roles/.

9. Avanpost IDM. URL: https://www.avanpost.ru/products/avanpost-idm/.

10. Oracle Identity Manager. URL: https://www.oracle.com/ru/middleware/technologies/identity-management-downloads.html.

11. 1IDM. URL : https://1idm.ru.

ОБ АВТОРАХ

ЗАБИРОВ Ильдар Исмагилович, магистрант 2-го курса ИБ-206м.

МАШКИНА Ирина Владимировна, докт. техн. наук, профессор кафедры ВТЗИ.

METADATA

Title: Applying of identification and access control management system in Industrial Control System

Affiliation: Ufa University of Science and Technology (UUST), Russia.

Email: [1] Ildar.zabirov.lord@mail.ru, [2] profmashkina@mail.ru

Language: Russian.

Source: Molodezhnyj Vestnik UGATU (scientific journal of Ufa University of Science and Technology), no. 1 (27), pp. 53-58, 2023. ISSN 2225-9309 (Print).

Abstract: It is proposed to reduce the load on the security administrator and ensure a higher level of information security to use systems in the ICS IdM/IAM that allow automating access rights management processes. The article provides a list of information entities: information objects and access subjects specific to the industrial network. A hierarchical scheme of user roles has been developed.

Key words: information assets; information subjects; access control; user account and rights management; hierarchy of users roles.

About authors:

ZABIROV Ildar Ismagilovich, 2nd year master student IB-206m, Ufa state aviation technical University.

MASHKINA Irina Vladimirovna, doc. tech. Sciences, professor of the department VTZI, Ufa state aviation technical University.