УДК 004.056
doi: 10.26583/bit.2024.3.06

Моханнад О. Заид Алкилани[1], Ирина В. Машкина[2]
Уфимский университет науки и технологий,
ул. К. Маркса, 12, Уфа, 450008, Россия
[1]*e-mail: muhannad.killani@gmail.com, https://orcid.org/0009-0003-9070-8968*
[2]*e-mail: profmashkina@mail.ru, https://orcid.org/0000-0002-3096-3102*

МОДЕЛЬ УПРАВЛЕНИЯ ДОСТУПОМ В АСУ ТП

Аннотация. Целью работы является разработка модели политики управления доступом и методики создания сценариев угроз информационной безопасности (ИБ) в автоматизированной системе управления технологическим процессом (АСУ ТП). Разработана политика управления доступом на основе задания ролей, в которой представлены сформированные в результате анализа технологических процессов информационные активы – объекты доступа, необходимые для функционирования промышленной сети, в также приведен специфичный для АСУ ТП уточненный перечень персонала – субъектов доступа, поддерживающих производственные технологические процессы. Построена иерархия ролей пользователей, в которой исключена роль суперпользователя, имеющего всю совокупность привилегий, разработана матрица разграничения доступа. Модель управления может быть использована при разработке частной политики разграничения доступа в рамках административных политик информационной безопасности. В работе сформулирована методика EPC-моделирования сценариев реализации угроз информационной безопасности, отражающая этапы направленных на целевые объекты АСУ ТП сложных многокомпонентных атак, когда киберпреступник осуществляет проникновение во внешнюю подсеть – бизнес-контур, а затем – во внутреннюю промышленную сеть, нарушая политику управления доступом. Приведен пример построения сценария угрозы OPC-серверу на основе EPC-диаграммы с указанием применяемых киберпреступником тактик и техник, приводящих к реализации угрозы безопасности информации из банка данных. Методика построения сценариев позволяет наглядно отобразить последовательность действий киберпреступника, связанных с использованием уязвимостей и техник, и результатов этих действий – событий, влияющих на развитие атаки. SIEM может быть настроена на обнаружение последовательности событий, выявленных с использованием EPC-моделирования. Разработанные сценарии будут способствовать своевременному обнаружению и адекватному реагированию на ранних этапах реализации кибератак.
Ключевые слова: автоматизированная система управления технологическим процессом АСУ ТП, субъекты доступа, объекты доступа, иерархия ролей пользователей, EPC-диаграмма, объект воздействия угрозы, безопасность информации, угрозы безопасности информации (УБИ).
Для цитирования: АЛКИЛАНИ, Моханнад О. Заид; МАШКИНА, Ирина В. МОДЕЛЬ УПРАВЛЕНИЯ ДОСТУПОМ В АСУ ТП. Безопасность информационных технологий, [S.l.], т. 31, № 3, с. 124–136, 2024. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1674. DOI: http://dx.doi.org/10.26583/bit.2024.3.06.

Muhannad O. Zaid Alkilani[1], Irina V. Mashkina[2]
Ufa University of Science and Technology,
K. Marx str., 12, Ufa, 450008, Russia
[1]*e-mail: muhannad.killani@gmail.com, https://orcid.org/0009-0003-9070-8968*
[2]*e-mail: mashkina.vtzi@gmail.com, https://orcid.org/0000-0002-3096-3102*

Access control model in ICS

Abstract: The purpose of this article is to develop a model for an access control policy and to formulate a method for creating a model of information security threat scenarios in industrial control system (ICS). The results of developing an access control policy model based on role assignment are presented. This model

encompasses the information assets derived from the analysis of technological processes – access objects that are vital for the functioning of the industrial network. In addition to that a specific and refined list of personnel access subjects – responsible for maintaining production technological processes within the ICS context is provided. Furthermore, a hierarchy of user roles has been constructed, wherein the role of a super user, possessing all privileges, has been excluded, and an access differentiation matrix has been developed. The model can be utilized in the development of a customized access differentiation policy within the scope of administrative policies of information security. The article formulates a way for EPC-modelling of scenarios depicting the implementation of information security threats. These scenarios outline the stages of complex multi-component attacks targeting the objects of the ICS. It depicts situations where cybercriminals infiltrate the external subnet – the enterprise network – and subsequently penetrate the internal industrial network, violating access management policies. An example illustrating the construction of a threat scenario targeting an OPC-server based on EPC-model is provided. This example delineates the tactics and techniques employed by cybercriminals, leading to the realization of a security incident from the Threats Data Bank. The method for constructing scenarios enables the visual representation of the sequence of actions undertaken by attacker. This sequence involves the exploitation of vulnerabilities and techniques, as well as the resultant events that influence the progression of the attack. SIEM (Security Information and Event Management) can be constructed to detect sequences of events identified using EPC-modeling. Therefore, the developed scenarios will contribute to timely detection and appropriate response during the early stages of cyberattack implementation.
Keywords: industrial control system (ICS), information subjects, information objects, access control, management of user accounts and rights, hierarchy of user roles, EPC-model, object of threat impact, information security, information security threats.
For citation: ALKILANI, Muhannad O. Zaid; MASHKINA, Irina V. Access control model in ICS. IT Security (Russia), [S.l.], v. 31, no. 3, p. 124–136, 2024. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1674. DOI: http://dx.doi.org/10.26583/bit.2024.3.06.

Введение

В настоящее время АСУ ТП (промышленная сеть) является частью корпоративной информационной системы промышленного предприятия. С точки зрения безопасности желательно отделение АСУ ТП от остальной части корпоративной информационной системы, поскольку самый высокий уровень зрелости автоматизации характеризуется проработанностью всех процессов управления производством, комплексным использованием новых информационных технологий. С целью обеспечения эффективности управления производством разработаны такие системы как ERP и MES, которые широко используются на современных промышленных предприятиях для автоматизации учета ресурсов, времени, выпускаемой продукции, постановки производственных задач. Они связывают АСУ ТП с самым верхним уровнем управления производством корпоративной информационной системы. Причем информационное взаимодействие осуществляется через глобальную сеть. В литературе отмечается, что используемые АСУ ТП, соединенные в настоящее время с бизнес-контуром, почти незащищены от внешних источников угроз [1–3].

Одной из широко обсуждаемых проблем в среде специалистов в области информационной безопасности является обеспечение защищенности АСУ ТП. Требования в отношении разработки, внедрения, эксплуатации системы защиты информации (СЗИ) АСУ ТП установлены в приказе ФСТЭК №31[1], при отнесении АСУ ТП к значимым объектам критической информационной инфраструктурой (КИИ), требования к СЗИ регламентируются приказами ФСТЭК № 235[2] и № 239[3].

[1]Приказ ФСТЭК России от 14.03.2014 № 31 (ред. от 15.03.2021).
[2]Приказ ФСТЭК России от 21 декабря 2017 г. № 235.
[3]Приказ ФСТЭК России от 25 декабря 2017 г. № 239.

При этом требования к защите информации, обрабатываемой в АСУ ТП, включают определение угроз безопасности информации и разработку модели угроз, включающей *актуальные* угрозы, на основе методики[4]. Актуальные угрозы определяются по результатам построения сценариев с учетом возможностей внешних и внутренних нарушителей, киберпреступника, с учетом анализа уязвимостей компонентов инфраструктуры и средств защиты, возможных способов реализации, тактик и техник, последствий нарушения свойств безопасности информации. Кроме того, при определении требований к СЗИ учитываются положения политик обеспечения информационной безопасности (ИБ). Исходным этапом проектирования системы защиты является определение типов субъектов доступа и объектов доступа, метода управления доступом, формирование правил разграничения доступа субъектов к объектам доступа, подлежащих реализации в АСУ ТП.

1. Актуальность исследований

При *разработке* СЗИ АСУ ТП важной задачей является необходимость учета большого количества векторов атак на целевые объекты воздействия промышленной сети. На *этапе эксплуатации* системы защиты необходимо выявление и блокирование угроз нарушения ИБ. Поэтому модель угроз, разработанная на основе установления возможных сценариев реализации, является основой для эффективной работы системы оперативного мониторинга и контроля защищенности. Разработанные сценарии необходимы для выявления предпосылок реализации угроз или их обнаружения на ранних этапах.

В настоящее время появились комплексы *мониторинга* несанкционированных изменений в компонентах инфраструктуры бизнес-контура и промышленной сети, *выявления* попыток эксплуатации уязвимостей, нарушения политики разграничения доступа. Для реализации функционала комплексы могут быть настроены на выявление нарушения предустановленной на объекте защиты политики управления доступом и этапов возможных сценариев кибератак [4–7].

Построение графических нотаций EPC при разработке моделей угроз нарушения безопасности АСУ ТП впервые было предложено в [8]. Однако при этом события и функции не были описаны в контексте использования терминологии, принятой позже в нормативном документе[4], а именно: тактики, техники, УБИ. В [9] приведены примеры сценариев атак, реализуемых в АСУ ТП, с учетом современной нормативной базы, однако сама методика построения сценариев и преимущества ее использования не сформулированы.

При этом любая реализуемая угроза – это нарушение принятой в защищаемой информационной системе политики безопасности, в частности политики управления доступом, поскольку совершение деструктивных воздействий становится возможным для киберпреступника после получения им тем или иным способом прав авторизованного пользователя. Поэтому корректная разработка административной политики управления доступом, а затем реализация ее без ошибок администрирования являются важнейшими задачами обеспечения безопасности защищаемой информации в АСУ ТП.

2. Модель политики безопасности и сценарии угроз как компоненты эффективной системы управления доступом и мониторинга информационной безопасности в АСУ ТП

Ролевая модель доступа – это основополагающий документ, четко определяющий необходимый набор прав доступа ко всем компонентам для каждой должности в АСУ ТП.

[4]Приказ ФСТЭК России от 05.02.2021 «Методический документ. Методика оценки угроз безопасности информации».

Контроль доступа к данным – это метод, используемый для регулирования доступа сотрудников к информационным ресурсам организации. Подход состоит в разделении множества сущностей, составляющих систему, на множество субъектов и множество объектов. Идея управления доступом на основе ролей проста: ограничить доступ пользователей к системам и данным только тем минимумом, который им необходим для выполнения их работы, и не более того – эта концепция называется принципом наименьших привилегий (Principle of Least Privilege, PoLP). В среде доступа роль пользователя в организации определяет конкретные сетевые разрешения, которые ему предоставляются [10].

Для эффективного контроля доступа в АСУ ТП необходимо определить субъекты, имеющие право доступа, начиная с критически важных ресурсов. Политика управления доступом включает выделение авторизованных пользователей, точное определение их разрешенного доступа на основе установления ролей в АСУ ТП. Модель управления доступом рассматривает ресурсы как объекты, а пользователей в качестве субъектов, инициирующих запросы на доступ. В работе определены специфичные для АСУ ТП объекты и субъекты доступа, перечни которых представлены в табл. 1 и 2.

Таблица 1. Набор информационных объектов

Множество объектов доступа	
Наименование	Обозначение
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 технологических процессов, Техническое задание (операционные маршруты, этапы операции)	o7
Настройки ПЛК (инструкции)	o8
Алгоритм управления ПЛК	o9
Управляющие сигналы контроллерам	o10
Данные 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 (точки тревоги, предельные значения)	o15
Сведения о сети (таблицы коммутации и маршрутизации)	o16
Конфигурационные файлы	o17
Подсистема генерации графических и текстовых отчетов	o18

Таблица 2. Набор информационных субъектов

Множество субъектов доступа	
Наименование	Обозначение
Руководитель	PY
ERP менеджер	ERP1
MES менеджер	MES1
ИБ руководитель	ISSUP
Начальник (производства)	N1
SCADA инженер	SE
Инженер-программист управления технологическим процессом	EPRO
Инженер-программист безопасности (специалист ИБ)	EIS
Специалист по контрольно-измерительным приборам	EUTI
Диспетчер	D
Технолог	TE
Оператор	OP
Инженер по обслуживанию технологического оборудования	ES
Специалист по обслуживанию измерительного оборудования	TM
Администратор безопасности	ISA
Администратор сети	NA
Администратор	ADM
Сотрудник	S

Исходными данными для формирования множеств информационных сущностей в работе являются наборы, сформированные авторами в [11]. Однако на основе детального анализа должностных инструкций и необходимых функциональных обязанностей сотрудников-пользователей промышленной сети, в множество субъектов доступа добавлены шесть информационных субъектов. На рис. 1 приведена разработанная (с учётом множества введённых информационных субъектов) иерархическая структура ролей пользователей АСУ ТП.

В табл. 3 приведена безопасная зона доступа в форме прямоугольной матрицы, где строки представляют субъекты доступа, столбцы – объекты доступа, а разрешенные операции (права) субъекта на объект заносятся в соответствующие ячейки. В матрице применяются следующие обозначения: *w* – write, записать; *r* – read, прочитать; *e* – execute, выполнить; *c* – create, создавать; *d* – delete, удалить.

Новизна разработанной модели политики управления доступом в АСУ ТП, базирующейся на ролевой модели разграничения доступа, заключается в:

- формировании специфичных для промышленной сети как перечня объектов доступа (включая информационные объекты, связанные с обеспечением безопасности), так и перечня субъектов доступа с учетом всего комплекса бизнес-задач;
- назначении двух максимальных ролей, которые имеют одновременно максимальные привилегии доступа в соответствии с должностными обязанностями этих ролей в бизнес-задачах, необходимых для поддержания производственных процессов в АСУ ТП, что позволяет исключить из иерархии ролей суперпользователя, имеющего право напрямую обращаться как к потокам данных промышленной сети, связанным с технологическим процессом, так и управлять конфигурационной информацией, связанной с обеспечением безопасности АСУ ТП.

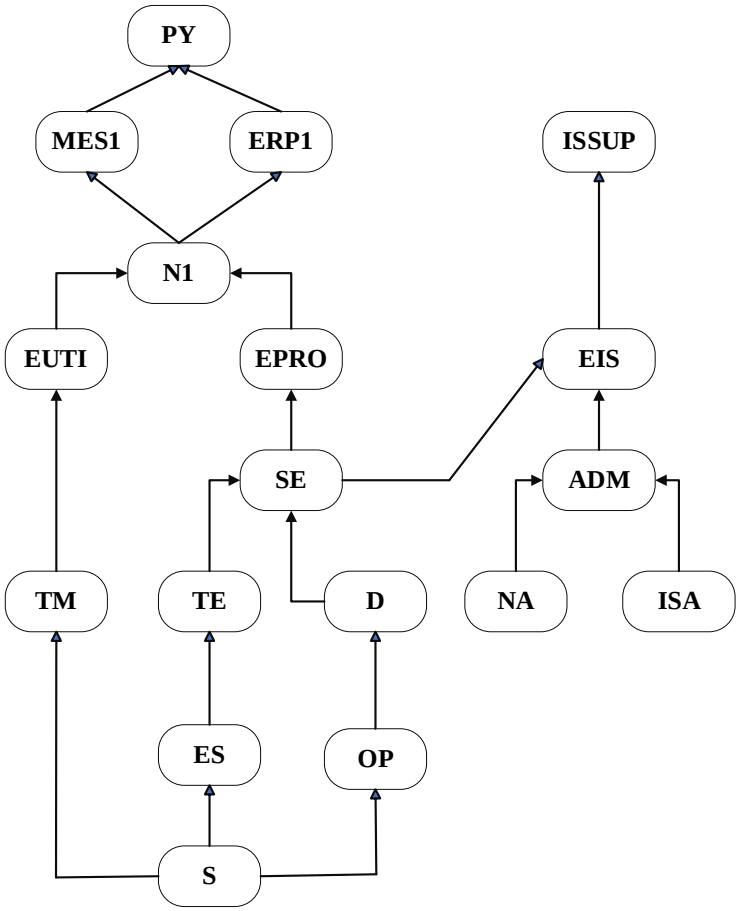

Рис. 1. Иерархическая структура ролей пользователей АСУ ТП

Полученные результаты определяют требования к параметрам настройки оборудования, программного обеспечения, включая программное обеспечение средств защиты информации, входящих в состав СЗИ АСУ ТП.

Уязвимости прикладных систем, в том числе систем диспетчерского контроля и сбора данных (SCADA), используемых для реализации бизнес-процессов в АСУ ТП, а также уязвимости, связанные с некорректно разработанными частными политиками ИБ, с некачественными подходами к администрированию коммуникационного оборудования и средств защиты, позволяют киберпреступнику выполнить проникновение как в бизнес-контур промышленного предприятия, так и в промышленную сеть.

В АСУ ТП важно осуществлять контроль и обнаруживать нарушение политики безопасности: непреднамеренные ошибочные действия операторов, администраторов, подозрительные действия персонала, активность киберпреступника по получению им прав доступа и привилегий авторизованного пользователя. Сценарии актуальных угроз безопасности, направленных на целевые объекты АСУ ТП, особенно в случаях сложных многокомпонентных атак, способствуют детектированию, по определенным признакам, действий нарушителей на ранних стадиях реализации сценария.

Таблица 3. Матрица разграничения доступа субъектов к объектам доступа

Обозначение	o1	o2	o3	o4	o5	o6	o7	o8	o9
PY	*rew*	*rew*	*re*	*rw*	*rw*	*re*	*rew*	*rew*	*rwecd*
ERP1	*rew*	*rew*	*re*	*rw*	*rw*	*r*	*rew*	*rew*	*rwecd*
MES1	*rew*	*rew*	*re*	*rw*	*rw*	*re*	*rew*	*rew*	*rwecd*
N1	*rew*	*rew*	*re*	*rw*	*rw*	*r*	*rew*	*rew*	*rwecd*
EUTI	*r*	*rew*	*r*	*r*	*r*	*r*	*r*	*re*	
TM		*r*	*r*	*r*	*r*	*r*	*r*	*re*	
EPRO	*rew*	*re*	*re*	*r*	*r*	*r*	*rew*	*rew*	*rwecd*
ISSUP	*rew*	*re*	*re*	*r*	*r*	*r*	*rew*	*re*	
EIS	*rew*	*re*	*re*	*r*	*r*	*r*	*rew*	*re*	
SE	*rew*	*re*	*re*	*r*	*r*	*r*	*rew*	*re*	
TE	*rew*	*re*	*re*	*r*	*r*	*r*	*rew*	*re*	
ES	*re*	*re*	*r*	*r*	*r*	*r*	*rew*	*r*	
D	*r*	*r*	*r*	*r*	*r*	*r*	*r*	*re*	
OP	*r*	*r*	*r*	*r*	*r*	*r*	*r*	*re*	
S		*r*		*r*	*r*				
ADM									
ISA									
NA									

Окончание таблицы 3

Обозначение	o10	o11	o12	o13	o14	o15	o16	o17	o18
PY	*rwe*	*r*		*rwe*	*rwe*	*rwe*			*rw*
ERP1	*rwe*	*r*		*rwe*	*rwe*	*rwe*			*rw*
MES1	*rwe*	*r*		*rwe*	*rwe*	*rwe*			*rw*
N1	*rwe*	*r*		*rwe*	*rwe*	*rwe*			*rw*
EUTI	*re*	*r*		*rw*	*r*	*r*			*rw*
TM	*r*	*r*		*rw*	*r*	*r*			*r*
EPRO	*rwe*	*r*			*rwe*	*rwe*			*rw*
ISSUP	*re*	*r*	*wre*		*re*	*re*	*rwecd*	*rwecd*	*r*
EIS	*re*	*r*	*wre*		*re*	*re*	*rwecd*	*rwecd*	*r*
SE	*re*	*r*			*re*	*re*			*r*
TE	*r*	*r*			*re*	*re*			*r*
ES	*r*	*r*			*re*	*re*			*r*
D	*re*	*r*			*re*	*re*			*r*
OP	*re*	*r*			*r*	*r*			*r*
S									*r*
ADM			*wre*				*rwed*	*rwecd*	
ISA			*r*				*r*	*re*	
NA			*r*				*re*	*r*	

Сценарии угроз могут оказать помощь специалистам службы ИБ в ходе идентификации угрозы, чтобы вовремя принять меры и осложнить возможное развитие

атаки, не допустив модификацию или уничтожение данных, отправку нелегитимной команды на ПЛК или другое деструктивное воздействие. Также сценарии дают ясное понимание того, какие события и логи нужны для анализа, включая средства защиты, SCADA, другое прикладное ПО, ПЛК, OPC.

В апреле 2022 г. исследователи в области кибербезопасности выявили новую угрозу для АСУ ТП. Эта угроза заключается в использовании деструктивного инструмента, названного Pipedream Incontroller (PI) [12]. Целью PI является получение доступа и контроля над атакуемым узлом в промышленной сети, что в конечном итоге позволяет киберпреступнику оказать разрушительное физическое воздействие на ТП. PI – это сложная многомодульная вредоносная программа, обеспечивающая возможность несанкционированного доступа киберпреступника в АСУ ТП для выполнения манипуляции на OPC-сервере [13].

Обычно технологию OPC применяют для обмена данными между контроллерами и SCADA системой, но также возможна организация сложных систем на разных уровнях АСУ ТП. OPC состоит из двух частей: OPC-клиента и OPC-сервера. ПО OPC-сервера через драйверы устройств по полевым шинам опрашивает различные устройства. ПО OPC-клиента обычно встроено в SCADA систему и предназначено для получения данных с OPC-сервера. OPC UA – это современный стандарт, описывающий передачу данных в промышленных сетях [14]. Произведя несанкционированный доступ к OPC-серверу, нарушитель получает возможность воздействия на ПЛК.

Прежде всего киберпреступник разворачивает канал скомпрометированного удаленного доступа в корпоративной сети. Далее злоумышленник использует инструмент для сбора учетных данных и получения доступа к легитимной учетной записи (Mimikatz). Создав устойчивый плацдарм в сети, используя канал (Dusttunnle), киберпреступник, просматривая сеть бизнес-контура, обнаруживает сегмент сети, разделяющий внутреннюю промышленную сеть (АСУ ТП) и бизнес-контур. С захваченными ранее учетными данными он может перемещаться в сети, компрометируя другие системы и ресурсы. На этом этапе киберпреступник может развернуть руткит (rootkit) – вредоносную программу, специально разработанную, чтобы оставаться скрытой, которая еще может отключить программы безопасности (Lazycargo). Это же вредоносное ПО может быть использовано на операторской станции для установки драйверов устройств, чтобы манипулировать трафиком между HMI и полевыми устройствами, используя уязвимости CVE-2020-15368 и CVE-2023-22655 [15].

Используя один из модулей PI для идентификации и доступа к серверу OPC-UA (метод перебора) в промышленной сети, киберпреступник может использовать атаку «человек посередине» [16], состоящую из двух компонентов: атака мошеннического сервера и атака мошеннического клиента. Для этого он создает OPC-клиент для подключения к реальному OPC-серверу, может собирать информацию о конечных точках в режиме реального времени. Киберпреступник затем предоставляет измененную информацию о техпроцессе легитимному клиенту OPC, что приводит к реальному нарушению техпроцесса и нанесению ущерба [16].

Рассмотрена возможность нарушения политики управления доступом к OPC-серверу киберпреступником, закрепившемся ранее в бизнес-контуре. В работе предложено для построения сценариев угроз ИБ АСУ ТП использовать графические нотации EPC, ключевыми элементами которых являются функции и события, связанные логическими операциями [17, 18]. Построена EPC диаграмма сценария реализации угрозы OPC-серверу, приведенная на рис. 2. Описание используемых киберпреступником уязвимостей приведено в табл. 4.

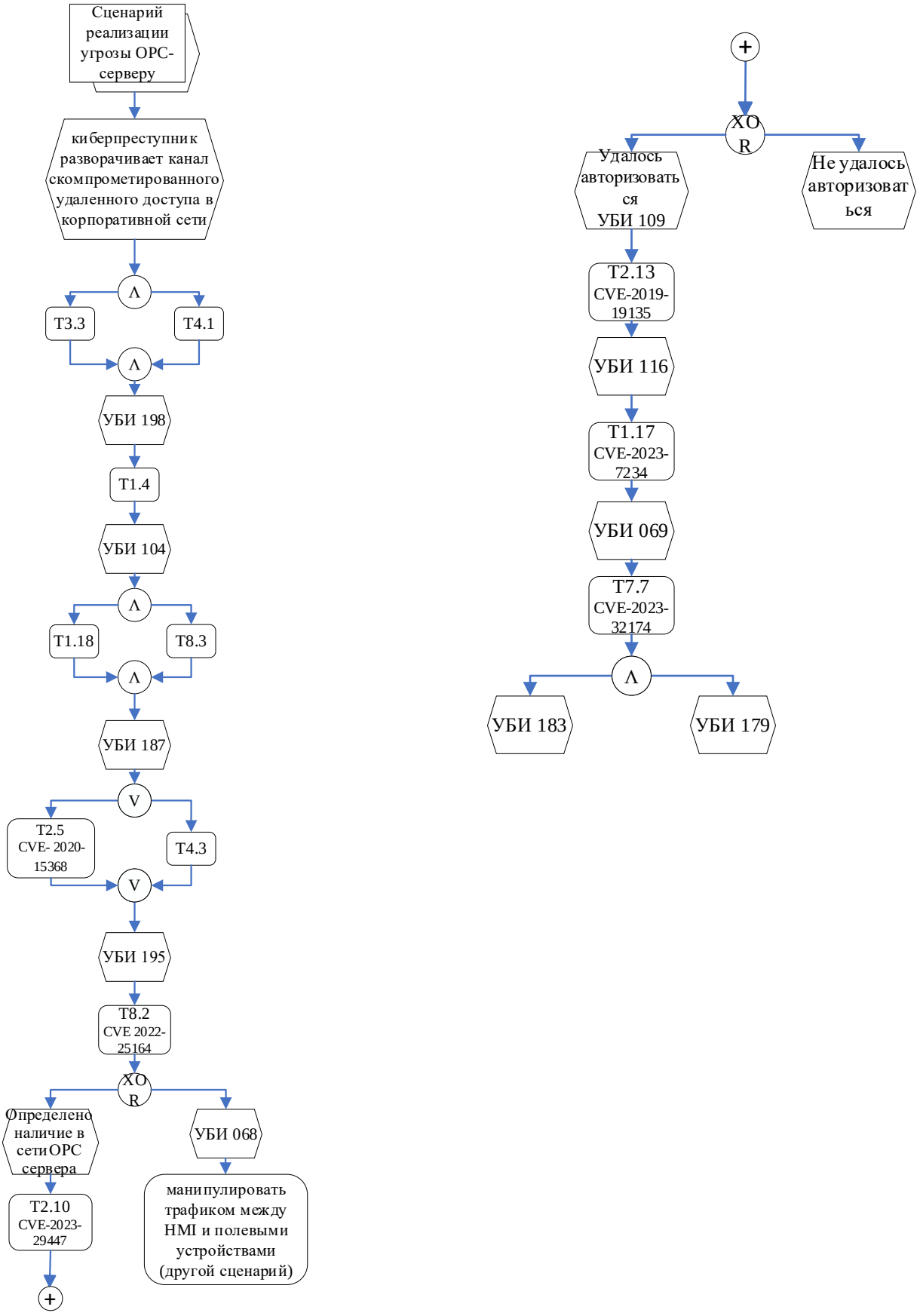

Рис. 2. EPC-диаграмма несанкционированного доступа к OPC-серверу

Таблица 4. Описание используемых киберпреступником уязвимостей

Тактика	Идентификаторы других систем описаний уязвимости	Описание уязвимости
T2.5	CVE-2020-15368 BDU:2022-02305	Уязвимость микропрограммного обеспечения драйвера материнской платы asRock AsrDrv103.sys, связанная с ошибками ограничения пользовательского пространства, позволяющая нарушителю выполнить произвольный код в ядре Windows.
T8.2	CVE 2022-25164 BDU:2022-07510	Уязвимость, позволяющая нарушителю получить ***доступ*** к модулю ЦП и ***модулю сервера OPC UA.***
T2.10	CVE-2023-29447 BDU:2023-05844	Уязвимость программного обеспечения OPC-серверов Kepware KEPServerEX и ThingWorkx Kepware Server, связанная с недостаточной защитой регистрационных данных, позволяющая ***нарушителю выполнить атаку типа "человек посередине".***
T2.13	CVE-2019-19135	Позволяет злоумышленникам «человек посередине» повторно использовать зашифрованные учетные данные пользователя, отправленные по сети.
T1.17	CVE-2023-7234	Инструментарий OPC-UA Server Toolkit запишет сообщение журнала после успешного подключения клиента OPC-UA, содержащее самоопределенное поле описания клиента (***начать контакт между клиентом и сервером OPC UA).***
T7.7	CVE-2023-32174 BDU:2023-09027	Уязвимость обработчика объектов NodeManagerOpcUa программного средства миграции серверов Unified Automation UaGateway, позволяющая нарушителю выполнить произвольный код (***OPC-сервер с полным контролем).***

Методика построения EPC-диаграммы сценариев угроз заключается в следующем:

- определение и задание целевого объекта: SCADA система, PLC-контроллер, АРМ оператора, АРМ администратора безопасности, АРМ инженера по управлению, OPC-сервер;
- выявление возможных для этапа тактик и соответствующих техник;
- поиск, выявление и анализ уязвимостей для их реализации;
- потенциально возможный результат использования киберпреступником техник обозначается как событие; поиск УБИ в базах данных[5, 6] ;
- построение логической цепочки взаимодействия функций и событий;
- достижение цели реализации сценария – объекта воздействия угрозы;
- EPC-диаграмму следует дополнить представленным в табличной форме описанием уязвимостей, используемых киберпреступником при реализации им каждой из техник сценария.

Методика построения сценариев угроз для оценки их актуальности с помощью EPC-диаграмм отличается наглядным графическим отображением целевого воздействия на информационную среду объекта защиты, детальностью этапов, представленных в виде цепочки процессов: действий или наборов действий, выполняемых киберпреступником, и событий как результатов этих действий, оказывающих влияние на развитие атаки.

[5]Банк данных УБИ ФСТЭК. URL: https://bdu.fstec.ru/threat (дата обращения: 25.04.2024).
[6]National vulnerability database. URL: https://nvd.nist.gov/ (дата обращения: 25.04.2024).

Заключение

Разработана модель политики управления доступом пользователей в АСУ ТП с учетом специфичных для промышленной сети объектов и субъектов доступа, поддерживаемых производственных процессов; в модели исключена роль суперпользователя, имеющего привилегии обращения как к информации, связанной с технологическим процессом, так и к конфигурационной.

Представлена методика построения сценариев угроз информационной безопасности, связанных с нарушением политики управления доступом к основным компонентам АСУ ТП. Приведен пример построения сценария угрозы OPC-серверу на основе EPC-диаграммы с указанием применяемых тактик и техник, приводящих к реализации УБИ из банка данных.

Разработанные EPC-диаграммы угроз будут способствовать своевременному обнаружению и оперативному реагированию на действия киберпреступника или внутреннего нарушителя. В частности, SIEM может быть *настроена* на выявление последовательностей событий, представленных в EPC-диаграммах, что позволит повысить уровень защищенности технологических процессов.

СПИСОК ЛИТЕРАТУРЫ:

1. Gaggero G.B., Armellin A., Portomauro G. and Marchese M. Industrial Control System-Anomaly Detection Dataset (ICS-ADD) for Cyber-Physical Security Monitoring in Smart Industry Environment. IEEE Access, v. 12, p. 64140–64149, 2024. DOI: 10.1109/ACCESS.2024.3395991.
2. Simon Burge. What is Industrial Control Systems Security. International security journal, June 7, 2023, ICO registration number: CSN0536342. URL: https://internationalsecurityjournal.com/industrial-control-systems/ (дата обращения: 25.04.2024).
3. Makrakis Georgios Michail & Kolias Constantinos & Kambourakis, Georgios & Rieger, Craig & Benjamin, Jacob. (2021). Vulnerabilities and Attacks Against Industrial Control Systems and Critical Infrastructures. URL: https://www.researchgate.net/publication/354493711_Vulnerabilities_and_Attacks_Against_Industrial_Control_Systems_and_Critical_Infrastructures (дата обращения: 25.04.2024).
4. Positive Technologies Industrial Security Incident Manager. описание продукта PT-ISIM 4. Продукт класса Industrial NTA/NDR для решения современных задач промышленного SOC. 2023. URL: https://www.ptsecurity.com/upload/corporate/ru-ru/products/isim/PT-ISIM-Data-Sheet-rus.pdf (дата обращения: 25.04.2024).
5. Анатолий Мухин. Обзор Kaspersky Industrial CyberSecurity for Networks. URL: https://www.anti-malware.ru/reviews/Kaspersky-Industrial-CyberSecurity-for-Networks (дата обращения: 25.04.2024).
6. Сергей Лыдин. Обзор DATAPK – комплекса оперативного мониторинга и контроля защищённости АСУ ТП. URL: https://www.anti-malware.ru/reviews/PAK-DATAPK (дата обращения: 25.04.2024).
7. Wahab Ahmed. (2023). SIEM TOOLS (Security Information and Event Management Tools as a field of Computer Security). URL: https://www.researchgate.net/publication/376955848_SIEM_TOOLS_Security_Information_and_Event_Management_Tools_as_a_field_of_Computer_Security (дата обращения: 25.04.2024). DOI: 10.13140/RG.2.2.24105.77929.
8. Машкина Ирина В.; Гарипов Ильдар Р. Разработка EPC-моделей угроз нарушения информационной безопасности автоматизированной системы управления технологическими процессами. Безопасность информационных технологий, [S.l.], т. 26, № 4, с. 6–20, 2019. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2019.4.01.
9. Заид Алкилани М.О., Машкина И.В. Разработка сценариев атак для оценки угроз нарушения информационной безопасности в промышленной сети. Проблемы информационной безопасности. Компьютерные системы. 2024, № 1(58), с. 96–109. DOI 10.48612/jisp/xvkx-k619-3f2z 25.04.2024. – EDN: PDNEWN.
10. Rostami G. Role-Based Access Control (RBAC) Authorization in Kubernetes. In Journal of ICT Standardization, v. 11, no. 3, p. 237–260, 2023. DOI: 10.13052/jicts2245-800X.1132.

11. Заид Алкилани М.О., Машкина И.В. Политика контроля доступа в автоматизированной системе управления технологическим процессом (АСУ ТП). 2023, Вестник УрФО № 2(48) с. 42–48. DOI: 10.14529/secur230203.
12. Nathan Brubaker, Keith Lunden, Ken Proska, Muhammad Umair, Daniel Kapellmann Zafra. Incontroller: New State-Sponsored Cyber Attack Tools Target Multiple Industrial Control Systems. URL: https://www.mandiant.com/resources/blog/incontroller-state-sponsored-ics-tool (дата обращения: 25.04.2024).
13. CHERNOVITE's PIPEDREAM Malware Targeting Industrial Control Systems (ICS). URL: https://www.headmind.com/fr/pipedream-incontroller-ics-specific-malware-attacks/ (дата обращения: 25.04.2024).
14. Tudor Covrig, Adrian-Vasile Duka, Ovidiu-Alexandru Roșca, Alexandru Ciobotaru, Liviu Miclea. Comparing Two Different Implementations of OPC UA Clients. April 2024. DOI: 10.1007/978-3-031-54674-7_15.
15. Pipedream: chernovite's emerging malware targeting industrial control systems. Dragos, Inc.April, 2022. URL: https://media.telefonicatech.com/telefonicatech/uploads/2021/1/154019_Dragos_ChernoviteWP_v2b.pdf (дата обращения: 25.04.2024).
16. Alessandro Erba, Anne Müller, and Nils Ole Tippenhauer. 2022. Security Analysis of Vendor Implementations of the OPC UA Protocol for Industrial Control Systems. In Proceedings of the 4th Workshop on CPS & IoT Security and Privacy (CPSIoTSec '22), p 1–13. Association for Computing Machinery, New York, NY, USA. DOI: https://doi.org/10.1145/3560826.3563380.
17. Guohua Xin. Research on EPC Construction Mode of China Informatization Project. Pacific International Journal 6(3):144-149, Sep 2023. DOI: 10.55014/pij.v6i3.428.
18. Medved P. EPC(HC) - energy performance contracting (EPC) model for historic city centres. Acta Innovations 47:28-40, January 2023. DOI: 10.32933/ActaInnovations.47.3.

REFERENCES:

[1] Gaggero G.B., Armellin A., Portomauro G. and Marchese M. Industrial Control System-Anomaly Detection Dataset (ICS-ADD) for Cyber-Physical Security Monitoring in Smart Industry Environment. IEEE Access, v. 12, p. 64140–64149, 2024. DOI: 10.1109/ACCESS.2024.3395991.
[2] Simon Burge. What is Industrial Control Systems Security. International security journal, June 7, 2023, ICO registration number: CSN0536342. URL: https://internationalsecurityjournal.com/industrial-control-systems/ (accessed: 25.04.2024).
[3] Makrakis Georgios Michail & Kolias Constantinos & Kambourakis, Georgios & Rieger, Craig & Benjamin, Jacob. (2021). Vulnerabilities and Attacks Against Industrial Control Systems and Critical Infrastructures. URL: https://www.researchgate.net/publication/354493711_Vulnerabilities_and_Attacks_Against_Industrial_Control_Systems_and_Critical_Infrastructures (accessed: 25.04.2024).
[4] Positive Technologies Industrial Security Incident Manager. Product description of THE SIMS 4. A product of the Industrial NTA/NDR class for solving modern problems of industrial SOC. 2023. URL: https://www.ptsecurity.com/upload/corporate/ru-ru/products/isim/PT-ISIM-Data-Sheet-rus.pdf (accessed: 25.04.2024) (in Russian).
[5] Anatoliy Mukhin. Obzor Kaspersky Industrial CyberSecurity for Networks. URL: https://www.anti-malware.ru/reviews/Kaspersky-Industrial-CyberSecurity-for-Networks (accessed: 25.04.2024) (in Russian).
[6] Sergey Lydin. Obzor DATAPK – kompleksa operativnogo monitoringa i kontrolya zashchishchonnosti ASU TP. URL: https://www.anti-malware.ru/reviews/PAK-DATAPK (accessed: 25.04.2024). (in Russian).
[7] Wahab Ahmed. (2023). SIEM TOOLS (Security Information and Event Management Tools as a field of Computer Security). URL: https://www.researchgate.net/publication/376955848_SIEM_TOOLS_Security_Information_and_Event_Management_Tools_as_a_field_of_Computer_Security (accessed: 25.04.2024). DOI: 10.13140/RG.2.2.24105.77929.
[8] Mashkina Irina V.; Garipov Ildar R. Development of EPC-Models of threats to information security of the automated process control system. IT Security (Russia), [S.l.], v. 26, no. 4, p. 6–20, 2019. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2019.4.01 (in Russian).
[9] Zaid Alkilani M.O., Mashkina I.V. Development of attack scenarios for assessing threats related to information security breach in industrial networks. 2024, no. 1(58), p. 96–109. DOI: 10.48612/jisp/xvkx-k619-3f2z (in Russian). – EDN: PDNEWN.

[10] Rostami G. Role-Based Access Control (RBAC) Authorization in Kubernetes. In Journal of ICT Standardization, v. 11, no. 3, p. 237–260, 2023. DOI: 10.13052/jicts2245-800X.1132.
[11] Zaid Alkilani M.O., Mashkina I.V. Politika kontrolya dostupa v avtomatizirovannoy sisteme upravleniya tekhnologicheskim protsessom (ICS). 2023, Vestnik UrFO № 2(48) s. 42–48. DOI: 10.14529/secur230203 (in Russian).
[12] Nathan Brubaker, Keith Lunden, Ken Proska, Muhammad Umair, Daniel Kapellmann Zafra. Incontroller: New State-Sponsored Cyber Attack Tools Target Multiple Industrial Control Systems. URL: https://www.mandiant.com/resources/blog/incontroller-state-sponsored-ics-tool (accessed: 25.04.2024).
[13] CHERNOVITE's PIPEDREAM Malware Targeting Industrial Control Systems (ICS). URL: https://www.headmind.com/fr/pipedream-incontroller-ics-specific-malware-attacks/ (accessed: 25.04.2024).
[14] Tudor Covrig, Adrian-Vasile Duka, Ovidiu-Alexandru Roșca, Alexandru Ciobotaru, Liviu Miclea. Comparing Two Different Implementations of OPC UA Clients. April 2024. DOI: 10.1007/978-3-031-54674-7_15.
[15] Pipedream: chernovite's emerging malware targeting industrial control systems. Dragos, Inc.April, 2022. URL: https://media.telefonicatech.com/telefonicatech/uploads/2021/1/154019_Dragos_ChernoviteWP_v2b.pdf (accessed: 25.04.2024).
[16] Alessandro Erba, Anne Müller, and Nils Ole Tippenhauer. 2022. Security Analysis of Vendor Implementations of the OPC UA Protocol for Industrial Control Systems. In Proceedings of the 4th Workshop on CPS & IoT Security and Privacy (CPSIoTSec '22), p1–13. Association for Computing Machinery, New York, NY, USA. DOI: https://doi.org/10.1145/3560826.3563380.
[17] Guohua Xin. Research on EPC Construction Mode of China Informatization Project. Pacific International Journal 6(3):144–149, Sep 2023. DOI: 10.55014/pij.v6i3.428.
[18] Medved P. EPC(HC) - energy performance contracting (EPC) model for historic city centres. Acta Innovations 47:28-40, January 2023. DOI: 10.32933/ActaInnovations.47.3.

Поступила в редакцию – 25 апреля 2024 г. Окончательный вариант – 22 июня 2024 г.
Received – April 25, 2024. The final version – June 22, 2024.