Ирина В. Машкина[1], Ильдар Р. Гарипов[2]
[1, 2]*ФГБОУ ВО «Уфимский государственный авиационный технический университет», ул. К. Маркса, 12, г. Уфа, 450008, Россия*
[1]*e-mail: mashkina.vtzi@gmail.com, https://orcid.org/0000-0002-3096-3102*
[2]*e-mail: ildar.garipov.92@mail.ru, https://orcid.org/0000-0002-0153-5459*

РАЗРАБОТКА EPC-МОДЕЛЕЙ УГРОЗ НАРУШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ

DOI: http://dx.doi.org/10.26583/bit.2019.4.01

Аннотация. Целью статьи является разработка моделей угроз, специфичных для объекта защиты – автоматизированных систем управления технологическими процессами (АСУ ТП). При разработке моделей угроз предлагается метод построения графических нотаций EPC (Event-driven Process Chain), основными элементами которых являются события и функции, связанные логическими операциями. В данной работе приведены результаты анализа угроз нарушения информационной безопасности автоматизированных систем управления технологическими процессами. Представлены EPC-модели угроз нарушения информационной безопасности современных информационно-управляющих систем промышленных предприятий. EPC-модели позволяют подробно описать пути реализации угроз, актуальных для современных АСУ ТП, что, в свою очередь, дает возможность специалистам, работающим в области информационной безопасности, проектировать системы защиты информации (СЗИ) в АСУ ТП, адекватные потенциальным угрозам и с учетом специфики производства. Моделирование угроз нарушения информационной безопасности (ИБ) позволяет специалисту по защите информации (ЗИ) получить достаточно убедительные доводы о возможности реализации нарушителем угроз конкретной АСУ ТП, что способствует финансированию проекта в необходимом объеме. В статье не ограничиваемся рассмотрением только моделей бизнес-процессов, как единственного средства создания моделей угроз в сфере информационной безопасности, а предлагаем EPC-моделирование, как один из методов построения угроз информационной безопасности АСУ ТП. EPC-модели позволяют описать пути реализации угроз, актуальных для современных АСУ ТП и оценить вероятности их реализации.

Ключевые слова: АСУ ТП, EPC-модель, информационная безопасность, АРМ, ERP, MES, информационная система, OPC, SCADA.
Для цитирования: МАШКИНА, Ирина В.; ГАРИПОВ, Ильдар Р. РАЗРАБОТКА EPC - МОДЕЛЕЙ УГРОЗ НАРУШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ. Безопасность информационных технологий, [S.l.], v. 26, n. 4, p. 6–20, 2019. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1172>. Дата доступа: 01 dec. 2019. doi:http://dx.doi.org/10.26583/bit.2019.4.01.

Irina V. Mashkina[1], Ildar R. Garipov[2]
[1, 2]*Ufa State Aviation Technical University, K. Marx street, 12, Ufa, 450008, Russia*
[1]*e-mail: mashkina.vtzi@gmail.com, https://orcid.org/0000-0002-3096-3102*
[2]*e-mail: ildar.garipov.92@mail.ru, https://orcid.org/0000-0002-0153-5459*

Development of EPC-Models of threats to information security of the automated process control system

DOI: http://dx.doi.org/10.26583/bit.2019.4.01

Abstract. The purpose of this study is to develop threat models specific to the object of protection-automated process control systems. When developing the threat models, we propose a method of

constructing graphical notations of events (Event-driven Process Chain), the main elements of which are events and functions associated with logical operations. We present the results of the analysis of threats of violation of information security of automated control systems of technological processes. The EPC-models of threats of information security violation of modern information and control systems of industrial enterprises are presented. The EPC-models allow to describe in detail ways of realization of the threats that, in turn, gives the chance to the experts working in the field of information security to design systems of information protection matched to potential threats and taking into account specifics of production. Modeling threats of violation of information security allows the specialist for data protection obtaining sufficient arguments about the feasibility of a violator of the threats to specific automated control systems of technological processes, which contributes to the financing of the project. This paper is not limited to the consideration of only business process models as the only means of creating threat models in the field of information security, and offer EPC-modeling as one of the methods of building information security threats for automated control systems. The EPC models allow to describe ways of realization of the threats actual for modern automated control systems and to estimate probabilities of their realization.

Keywords: ICS, EPC model, information security, PC, ERP, MES, information system, OPC, SCADA.
For citation: 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, n. 4, p. 6–20, 2019. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1172>. Date accessed: 01 dec. 2019. doi:http://dx.doi.org/10.26583/bit.2019.4.01.

Введение

Информационные технологии и информационные системы (ИС) применяются в настоящее время во всех сферах жизнеобеспечения государства. По целевому назначению ИС подразделяются на два класса: информационно-организационные и информационно-управляющие (ИУС). ИУС предназначены для управления техническими объектами; на основе анализа характеристик протекающих в них процессов система формирует управляющие воздействия. АСУ ТП на производстве – это разновидность ИУС, требующая для выполнения определенных функций управления затрат труда операторов, включающая технические средства, которые обеспечивают замену физического и умственного труда человека работой машин для сбора, переработки и вывода информации [1].

Основное функциональное назначение АСУ ТП – это создание условий для работы и ведения бизнеса, автоматизация труда людей. АСУ ТП имеют многоуровневую структуру: уровень операторского (диспетчерского) управления (верхний уровень); уровень автоматического управления (средний уровень); уровень исполнительных устройств, а также ввода, вывода данных (нижний уровень) [2].

Безопасность АСУ ТП заключается в формировании и поддержании таких условий функционирования системы, при которых качество управления технологическим процессом не приведет к недопустимому ущербу самому технологическому комплексу, окружающей среде или людским ресурсам. Условия функционирования АСУ ТП должны обеспечивать защищенность системы от угроз нарушения конфиденциальности информации, циркулирующей на верхнем уровне, угроз нарушения целостности её на среднем и нижнем уровнях, а также от угроз нарушения доступности информационных сервисов для персонала.

Ранее считалось, что АСУ ТП сами по себе являются сложными для взлома системами в связи с использованием специфичного оборудования и программного обеспечения, однако с приходом современных технологий все изменилось. Развитие современных технологий привело к тому, что в современных системах управления для сокращения расходов на разработку и внедрение стали использоваться широко

распространенные операционные системы, сетевое оборудование и сетевые протоколы, которые имеют недостатки в виде уязвимостей.

1. Актуальность исследований

АСУ ТП стали присущи практически все уязвимости современных информационных систем. В компонентах, применяемых для управления технологическими процессами на промышленных объектах, в 2017 году были обнаружены более сотни уязвимостей [3]. Используя общедоступные поисковые системы, потенциальные злоумышленники могут удаленно получить доступ к компонентам АСУ ТП, в том числе к 4,5 тысячам устройств, обеспечивающих работу энергетических объектов во всем мире. Практически половина выявленных в 2017 году уязвимостей имеет высокий уровень, причем наибольшее количество уязвимостей найдено в продуктах самых известных производителей. Проведено исследование наличия открытых портов компонентов АСУ ТП, которые доступны через сеть Интернет. Исследование показало, что на одном критически важном объекте может быть до 50 тысяч открытых портов компонентов АСУ ТП, которые позволяют злоумышленнику осуществить атаку на систему и нарушить доступность компонента АСУ ТП [3].

Наибольшее количество уязвимостей найдено в SCADA-системах (43%), в специализированных сетевых устройствах (28%), в инженерном ПО диспетчерского и операторского контуров АСУ ТП (19%), в PLC (17%). Причем 47% процентов перечисленных уязвимостей имеют высокий уровень, и лишь 14% от заявленных специалистами уязвимостей устраняются в течение трех месяцев после обнаружения [3–4].

В [4] отмечается, что треть используемых АСУ ТП, соединенных с бизнес-контуром, почти не защищены от внешних источников угроз.

В настоящее время многие промышленные предприятия включают сегменты АСУ ТП в состав корпоративных информационных систем (КИС). Конечно, с точки зрения безопасности, желательна сегрегация АСУ ТП от остальной части КИС. Однако, известно, что промышленная сеть АСУ ТП может являться частью КИС предприятия. Дело в том, что самый высокий уровень зрелости автоматизации характеризуется проработанностью процессов управления производством, способностью АСУ ТП к быстрой адаптации при изменениях в бизнес-процессах, комплексным использованием новых информационных технологий. С целью обеспечения эффективности управления производством за счет повышения оперативности, то есть сокращения длительности цикла управления, разработаны такие системы как Enterprise Resource Planning (ERP) и Manufacturing Execution System (MES) [5, 6].

На современных промышленных предприятиях внедряются или уже используются системы учета ресурсов предприятия ERP и MES. Использование этих систем дает возможность автоматизировать учет используемых: ресурсов, времени и выпускаемой продукции. Кроме того, при помощи выше упомянутых систем проводится постановка производственных задач (например, для каждого цеха промышленного предприятия свой производственный план в определенных временных рамках). ERP и MES системы на промышленных предприятиях имеют непосредственную связь с верхним уровнем АСУ ТП и другими сегментами КИС [7].

Проблема обеспечения информационной безопасности АСУ ТП является одной из актуальных на сегодняшний день. Решение этой проблемы невозможно без разработки модели существенной среды, в которой функционирует СЗИ АСУ ТП, то есть без исследования и построения модели угроз нарушения ИБ. Успех создания СЗИ АСУ ТП в значительной мере зависит от адекватности модели существенной среды тем

дестабилизирующим факторам, которые влияют на функционирование объекта защиты – АСУ ТП.

2. Анализ АСУ ТП как объекта защиты

В статье рассматривается вариант с подключением АСУ ТП к информационной системе предприятия, который требует большего внимания специалистов по обеспечению информационной безопасности.

На рис. 1 представлена обобщенная архитектура сегмента КИС с АСУ ТП.

На периметре сегмента КИС с АСУ ТП используются маршрутизатор интернет и межсетевой экран, которые зарезервированы на случай сбоя. За кластером межсетевых экранов расположена демилитаризованная зона с общедоступными серверами (web, e-mail и т.д.). Внешняя подсеть сегмента включает в себя рабочие станции и сервера бизнес блока промышленного предприятия, сотрудники которого не имеют непосредственного доступа к информационным ресурсам АСУ ТП. К внешней подсети могут относиться локальные сетевые сегменты, например, конструкторского, технологического отделов, отдела планирования, разработки программного обеспечения или другие. Внутренняя подсеть, включающая в себя рабочие станции и сервера АСУ ТП, отделена от внешней подсети дополнительным кластером межсетевых экранов.

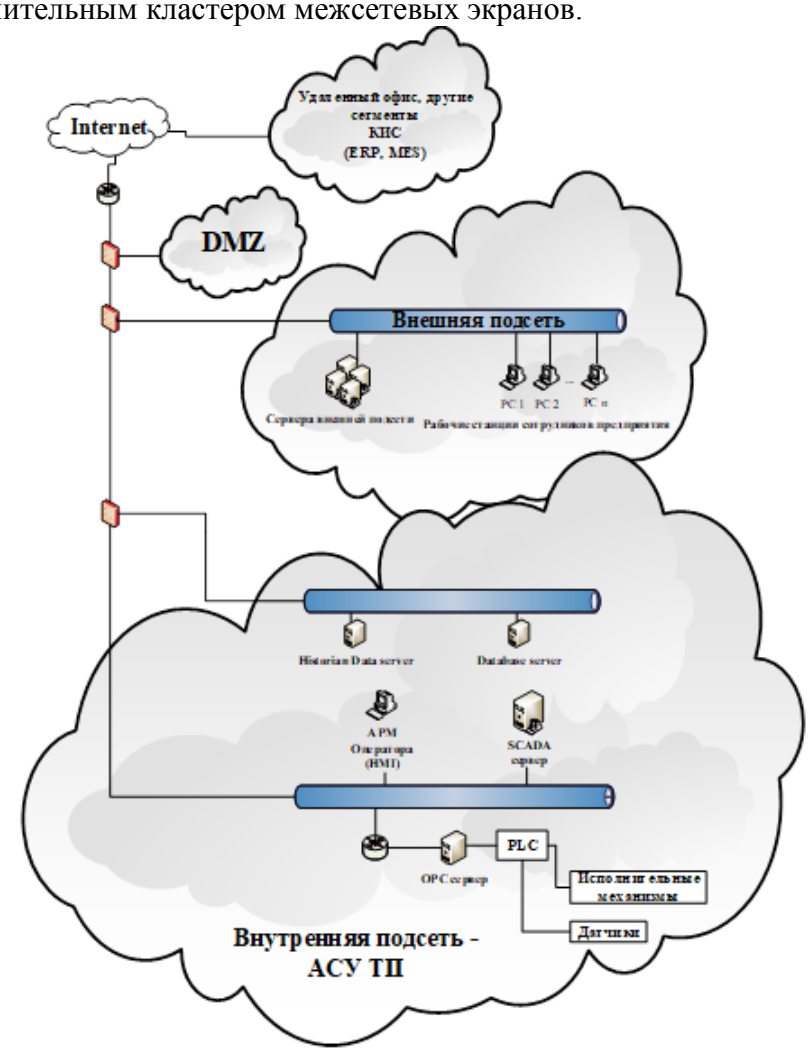

Рис. 1. Обобщенная архитектура сегмента КИС с АСУ ТП
(Fig. 1. General architecture segment is CIS with ICS)

Сервера, обрабатывающие информацию ограниченного доступа, предназначенную для обеспечения производственного процесса в АСУ ТП, расположены в экранированной подсети сегмента КИС (Historian Data Server и Database Server) и во внутренней подсети (SCADA, OPC).

На верхнем уровне АСУ ТП расположены средства вычислительной техники: сервера баз данных, сервера SCADA, автоматизированные рабочие места операторов (диспетчеров). На верхнем уровне производится обработка поступающих с нижнего уровня данных. Обработка данных подразумевает под собой: структурирование, архивирование и последующее хранение, предоставление данных операторам и диспетчерам для работы с ними при помощи человеко-машинного интерфейса (HMI – Human-Machine Interface). На верхнем уровне АСУ ТП помимо обработки данных с нижнего уровня реализуется функции управления.

На среднем уровне (уровне автоматического управления) расположены средства автоматизации, такие как программируемые логические контролеры (PLC).

На нижнем уровне расположены исполнительные устройства и датчики. В качестве исполнительных устройств могут выступать сервоприводы, электромоторы, насосы и механизмы, которые используются в различных видах производства. Для получения данных о протекании технологических процессов используются различного рода датчики и иные устройства съема информации. Состав, количество уровней АСУ ТП и выполняемые целевые функции зависят от назначения системы, определяются спецификой производственных технологических процессов.

К основным уязвимостям современных АСУ ТП эксперты относят [2, 3]:

- отсутствие или слабая защита от несанкционированного доступа к системам автоматизированного управления (пароли, персональные идентификаторы);
- недекларированные возможности SCADA-систем (систем диспетчерского управления и сбора данных);
- использование беспроводных коммуникаций (незащищенные беспроводные соединения);
- отсутствие чётких границ между разными сегментами сети (например, между корпоративными и промышленными);
- использование дистанционных методов управления (возможно по незащищенным каналам связи);
- несвоевременное или некорректное обновление программного обеспечения;
- отказ от минимальных мер безопасности (так как, нередко ради удобства и производительности компании отказываются от установки не только, например, антивирусной, но и даже парольной защиты критически важных активов);
- распространение Windows в качестве основной операционной системы для рабочих станций и даже для серверов;
- web-технологии, используемые на верхнем уровне АСУ ТП (если таковые используются, к примеру, в HMI).

Ниже представлен перечень основных угроз информационной безопасности АСУ ТП, отмеченных в реальных инцидентах [4]:

- атаки на узлы управления;
- атаки на SCADA-системы;
- атаки на программируемые логические контроллеры (PLC) с использованием уязвимостей самих PLC (пароль по умолчанию, неавторизованный доступ к фирменному программному обеспечению, удалённое изменение пароля и т.д.);

• атаки с использованием уязвимостей протоколов, используемых в информационно-управляющей системе предприятия (OPC – переполнение буфера, уязвимости протоколов TCP/IP);

• атаки на базы данных промышленных систем (несанкционированный доступ, SQL инъекции).

Реализация перечисленных выше угроз может привести к необратимым последствиям, таким как: отказ промышленного оборудования (неправильная работа оборудования, отказ системы управления и т.д.); техногенные катастрофы (аварии на производстве); человеческие жертвы (среди сотрудников и гражданского населения); экологические катастрофы (загрязнение окружающей среды); материальные и финансовые потери для предприятия или государства.

Перед построением СЗИ АСУ ТП необходимо определить, от чего, собственно, необходимо защищать информацию, то есть построить модель угроз данному конкретному объекту защиты. Модель угроз должна включать в себя перечень потенциально возможных угроз с учетом принятой политики безопасности, которые могут воздействовать на информацию в процессе ее обработки. Таким образом, принципиальной особенностью проблемы защиты информации в АСУ ТП является требование полноты определения возможных угроз информации, циркулирующей в инфраструктуре объекта защиты с учетом *специфических уязвимостей*. *Преднамеренные* угрозы являются основным фактором, который необходимо учитывать при проектировании СЗИ. В работе предлагается создание модели угроз на основе классификационной схемы угроз, приведенной в [8]. Моделирование угроз является по существу единственным методом достаточно полного исследования потенциально возможных деструктивных воздействий на информационную среду АСУ ТП. При моделировании преднамеренных угроз необходимо стремиться к полноте описания всех возможных путей их проникновения, с учетом множества возможных механизмов их реализации.

Все информационные системы проектируются на одних и тех же принципах (инфраструктура, сетевые протоколы), поэтому имеют практически одинаковые причины успешности реализации преднамеренных угроз: неверно разработанная политика разграничения доступа, отсутствие барьера на пути реализации атаки, неправильные настройки коммуникационного оборудования и средств защиты, уязвимости программного обеспечения. В работе предлагается каждую угрозу нарушения ИБ АСУ ТП рассматривать как сложную последовательность действий и событий, возникающих в процессе функционирования объекта защиты, приводящих его в подмножество ситуаций, при которых становятся возможными несанкционированный доступ или деструктивные изменения информационной среды. При использовании в атакуемой АСУ ТП криптографических протоколов, противник на основе методов криптоанализа и некоторых предположений проводит атаку на криптосистему. Совокупность таких атак постоянно расширяется за счет развития теоретических методов криптоанализа и возможностей техники. В основном атаки на криптосистему оказываются успешными только при оплошностях, допущенных при реализации криптосистем.

Сканирование и выявление открытых портов может позволить злоумышленнику идентифицировать активные сервисы и использовать их уязвимости. Получив доступ к информационной среде сегмента КИС с АСУ ТП, злоумышленник может пытаться реализовать фильтрацию информации идентификации–аутентификации. В результате её перехвата становится возможным выделение паролей из общего потока. В результате перебора уязвимостей возможно получение входа на узел сети. Полученный в результате этих действий доступ может иметь различный уровень. Злоумышленник может получить

доступ как пользователь, наделенный незначительными правами, в этом случае будет производиться попытка осуществления сборки «мусора» на жестком диске и оперативной памяти. Результатом может быть получение аутентификационной информации, позволяющей организовать более высокий уровень доступа, на котором злоумышленник может внедрить мобильный вредоносный код, позволяющий собирать или уничтожать требуемую информацию, осуществлять несанкционированный доступ к требуемой информации или даже изменять базы данных защиты (настроек), что позволит создать учетные записи несуществующих пользователей, обладающих правами доступа. При появлении у злоумышленника возможности модификации передаваемых данных (текстовых или исполняемый код) он может воздействовать на целостность исполняемого кода или внедрить вредоносное программное обеспечение (ВПО), которое позволит ему, после передачи пакета на сервер, воздействовать на программу аутентификации пользователей в базе данных и получить высокие права.

3. Результаты исследований

Разработанные модели угроз в АСУ ТП отображают ориентацию вектора распространения носителя при реализации угрозы на множестве компонентов инфраструктуры объекта защиты, месторасположение источника информации (SCADA, OPC, PLC, АРМ оператора), последовательность реализации атаки и используемые уязвимости, а также возможного нарушителя.

Целевые точки инфраструктуры АСУ ТП, на которые направлены векторы атак: автоматизированное рабочее место оператора – диспетчера (далее по тексту АРМ оператора), SCADA сервера и программируемые логические контроллеры (PLC). В том числе, часто в современных системах управления технологическими процессами используются OPC сервера.

В настоящей работе для моделирования угроз нарушения информационной безопасности АСУ ТП используются графические нотации EPC (Event-Driven Process Chain, событийная цепочка процессов), ключевыми элементами которой являются События и Функции, связанные между собой логическими операциями [9]. Для ветвления процесса используются логические отношения, описываемые символами «И» (/\), «включающее ИЛИ» (\/) и «Исключающее ИЛИ» (XOR). EPC-модели позволяют детально описать целенаправленные угрозы нарушения ИБ современных АСУ ТП. Рассмотрим построенную при помощи EPC-диаграмм модель угрозы подмены злоумышленником программ управления PLC на АРМ Оператора. На рис. 2 представлена EPC-модель угрозы нарушения ИБ АСУ ТП, когда злоумышленник проникает за периметр сегмента КИС с АСУ ТП путем заражения компьютера удаленного рабочего места ВПО, при помощи которого были скомпрометированы данные идентификации и аутентификации пользователя, имеющего доступ к некоторым серверам внешнего сегмента сети промышленного предприятия.

Разберем сценарий атаки, EPC-модель которой представлена на рис. 2.

Злоумышленник заразил ВПО (трояном) компьютер сотрудника промышленного предприятия, работающего с удаленного рабочего места. Троянская программа собрала данные со скомпрометированного узла (логины, пароли и данные, необходимые для связи узла с сервером промышленного предприятия по каналу VPN), далее злоумышленник создал на своем компьютере (при помощи украденных данных) копию скомпрометированного узла и произвел попытку подключения к серверу промышленного предприятия. После успешной авторизации на сервере злоумышленник определяет директорию, в которой хранятся хэш-суммы паролей пользователей, имеющих доступ к

этому серверу, в большинстве случаев это связано с неправильной настройкой прав доступа пользователей к ресурсам на серверах баз данных.

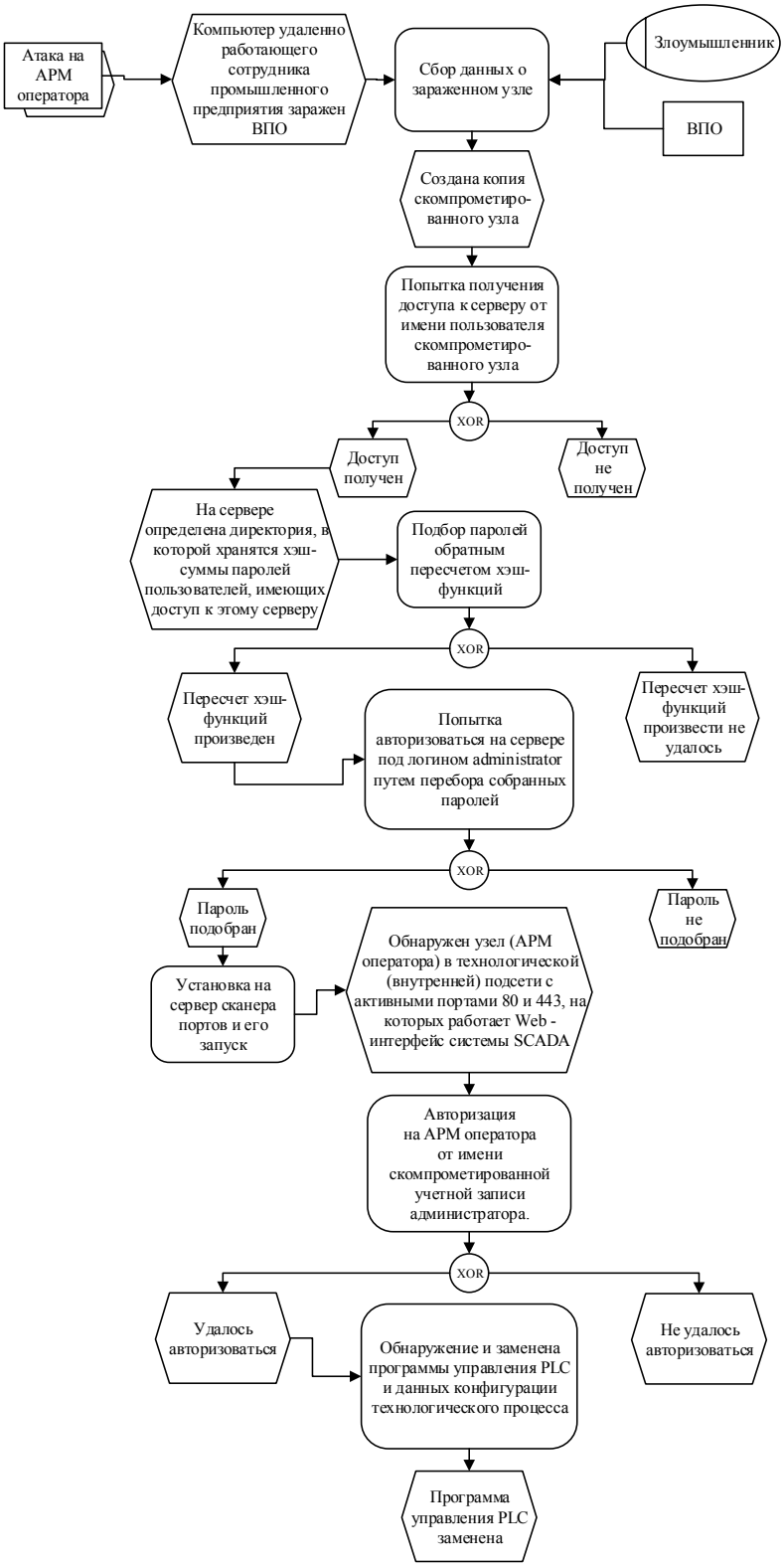

Рис. 2. EPC-модель угрозы замены на АРМ оператора программ управления PLC
(Fig. 2. EPC-model threat is the replacement for the PC operator programs the PLC control)

Злоумышленник произвел подбор паролей обратным пересчетом хэш-функций и попытался авторизоваться на сервере под логином administrator путем перебора собранных паролей. После того как атакующий подобрал пароль к логину administrator, он загрузил на сервер сканер портов и запустил его. Обнаружив узел (АРМ оператора) во внутренней (технологической) подсети с активным портом, на котором работает программное обеспечение Siemens SIMATIC WinCC, злоумышленник пытается авторизоваться на найденном узле от имени скомпрометированной учетной записи администратора.

Далее злоумышленник, обнаружив, заменил программы управления PLC и данные конфигурации технологического процесса на АРМ оператора. Итогом произведенной атаки стала ситуация, при которой программы управления PLC были заменены.

На данном примере представлена EPC-модель, по которой видно, что злоумышленник, получив доступ к сетевой инфраструктуре предприятия, производит: сканирование локальной вычислительной сети (ЛВС) на наличие уязвимостей (например, открытых портов, через которые работают сетевые сервисы программ и средств автоматизации) и сбор информации – при этом ему могут стать доступны данные учетных записей некоторых сотрудников предприятия. Злоумышленник может попытаться повысить привилегии пользователя, данные учетной записи которого были перехвачены и использовались в ходе атаки, до достаточного уровня для того, чтобы перехватить управление не только над определенным атакованным узлом, но и сетевым сервисом того или иного корпоративного приложения.

Настроив удаленный доступ к узлу ЛВС, управление над которым было перехвачено, злоумышленник может загружать, выгружать и изменять некоторую служебную информацию, например, файлы конфигурации, управляющие программы, данные телеметрии и так далее.

Подобного рода действия злоумышленников могут привести к непредсказуемым, иногда даже катастрофическим последствиям, от аварии на производстве, из-за которой промышленное предприятие понесет материальный ущерб, до экологической катастрофы с человеческими жертвами среди сотрудников и гражданского населения, в случае если производство было связано с опасными для экологии веществами.

Рассмотрим пример, в котором атакованным узлом сети стал SCADA-сервер. (рис.3). SCADA-сервер является основным звеном автоматизированной системы управления технологическими процессами. Перехват злоумышленником управления над данным узлом может привести к весьма негативным последствиям на производстве или там, где используется атакованная АСУ ТП, начиная с экстренной или аварийной остановки технологического процесса и заканчивая техногенной катастрофой.

Зачастую бывает, что SCADA-сервер и АРМ оператора – это одна вычислительная машина.

Рассмотрим пример сценария атаки, EPC-модель которой представлена на рис. 3.

На АРМ оператора злоумышленник установил сканер портов и сниффер пакетов, после чего, просканировав сеть, он определил наличие в ней SCADA-системы Siemens SIMATIC WinCC.

На примере уязвимости CVE-2014-8551 злоумышленник произвел запуск произвольного кода, без авторизации на сервере, с целью изменить конфигурацию SCADA-системы.

Рассмотрим описание уязвимости CVE-2014-8551. Сервер WinCC позволяет злоумышленникам выполнять произвольный код без прохождения авторизации [10].

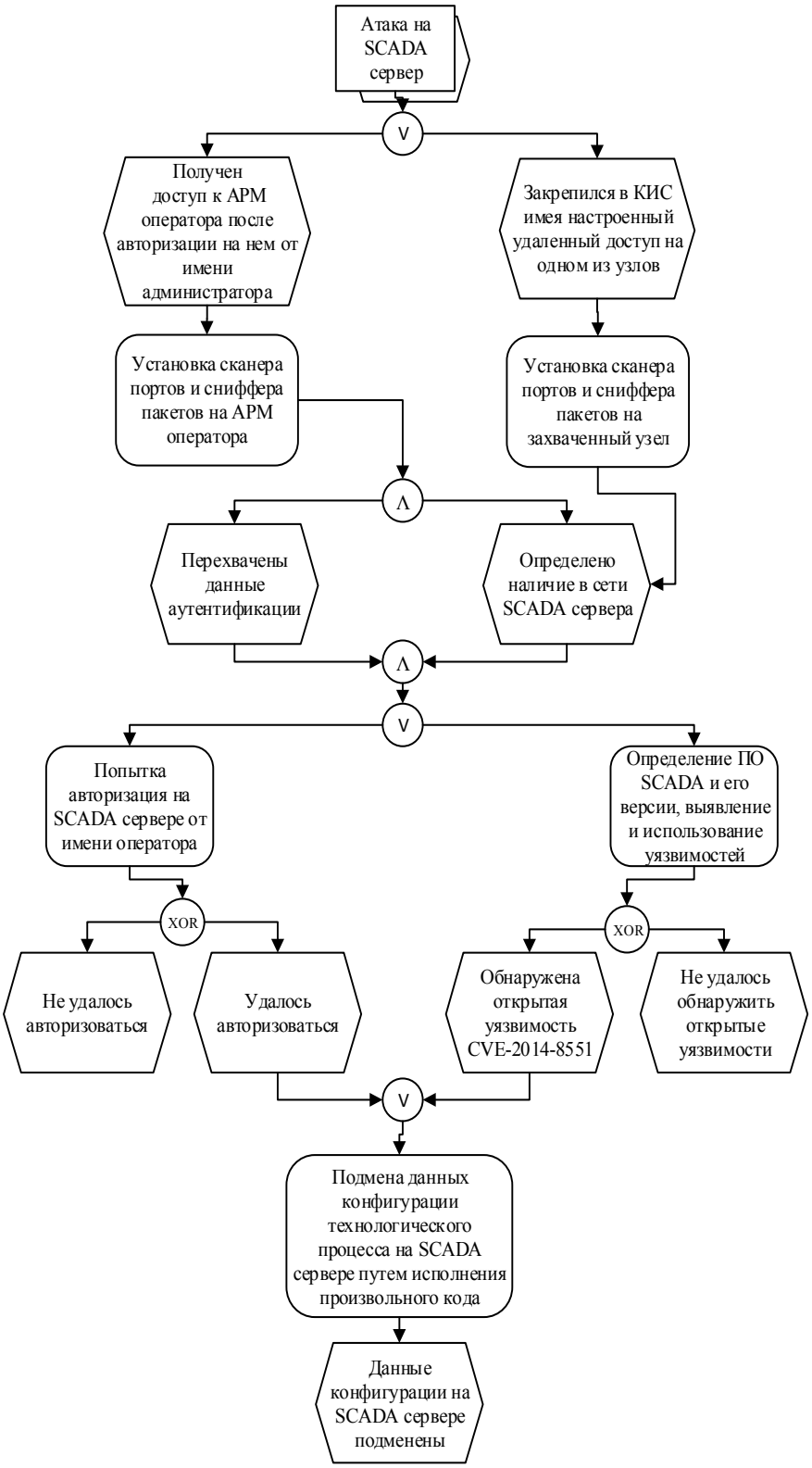

Рис. 3. EPC-модель угрозы нарушения информационной безопасности SCADA-сервера (Fig. 3. EPC-model of threat of violation of information security of SCADA-server)

Внесенные изменения могут нанести вред нормальному протеканию технологического процесса, что в дальнейшем может привести к отказу техники и даже аварии на производстве.

Рассмотрим пример, в котором атакованным узлом сети стал OPC-сервер (рис. 4).

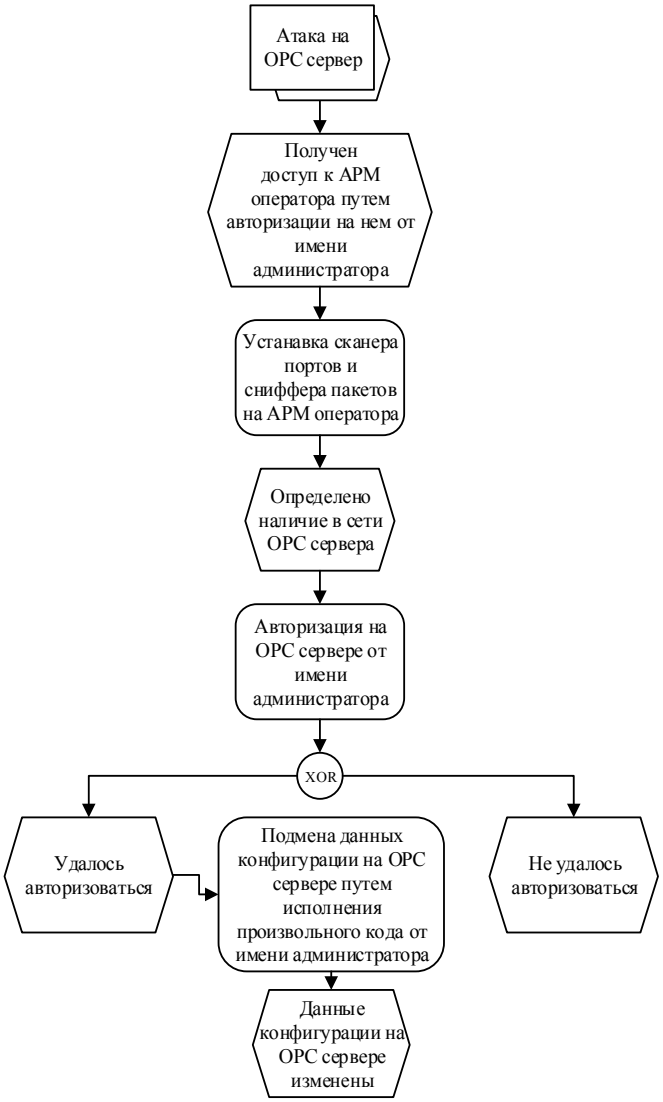

Рис. 4. EPC-модель угрозы нарушения информационной безопасности OPC-сервера (Fig. 4. EPC-model of threat of violation of information security of the OPC-server)

Назначение OPC-технологии – предоставить разработчикам промышленных программ универсальный интерфейс обмена данными с любыми устройствами разных производителей, использующих разные технологии передачи и предоставления данных. Функционирование OPC базируется на основе клиент-серверной технологии информационного взаимодействия, где клиентом сервера OPC является сервер управления SCADA. OPC-сервер играет важную роль в процессе обмена данными между средним и верхним уровнями АСУ ТП, поэтому его безопасность должна быть реализована на должном уровне.

Произведя несанкционированный доступ к OPC-серверу, злоумышленник может подменить данные, передаваемые между PLC и SCADA-сервером, а нарушение работы OPC-сервера может привести к потере связи между уровнями АСУ ТП.

Рассмотрим сценарий атаки, EPC-модель которой представлена на рис. 4.

Злоумышленник, получил доступ к АРМ оператора, произвел кражу данных учетной записи оператора и зафиксировался во внутренней подсети, настроив удаленный доступ. Просканировав сеть, определил в ней наличие OPC-сервера, злоумышленник авторизовался на OPC-сервере от имени администратора (логин и пароль которого были похищены ранее), далее он, получив доступ, от имени администратора на OPC-сервере изменил конфигурации взаимодействия SCADA-системы и PLC.

Рассмотрим пример, в котором атакованным узлом сети стал PLC (рис. 5).

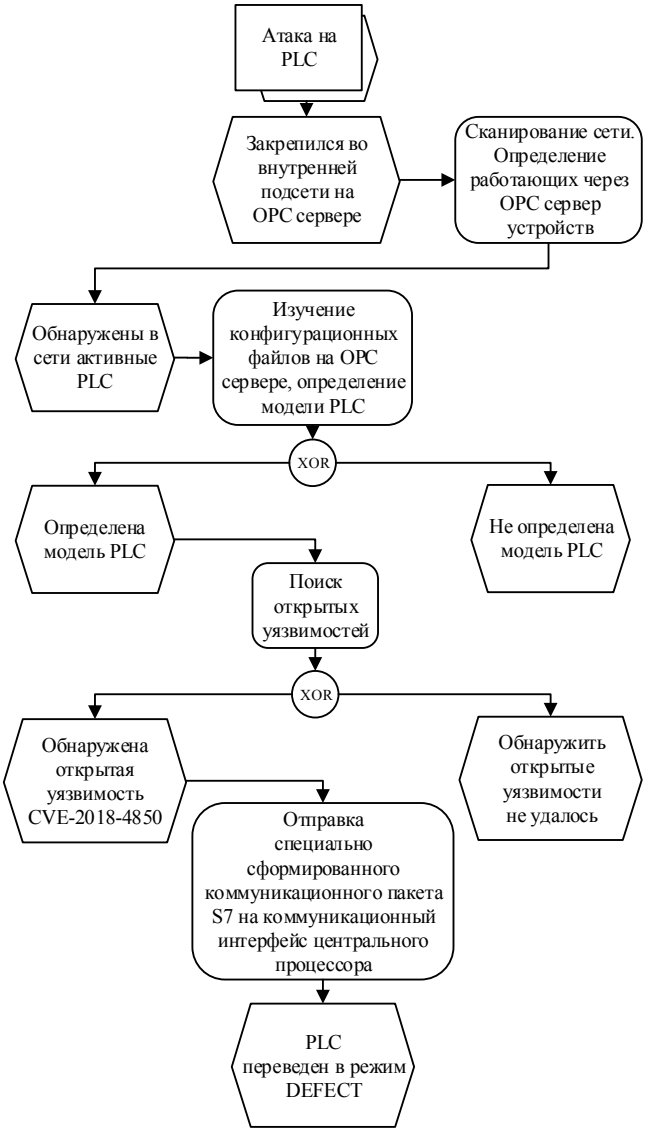

Рис. 5. EPC-модель угрозы нарушения информационной безопасности PLC
(Fig. 5. EPC-model of threat of violation of information security of PLC)

PLC – это устройство, используемое для автоматизации технологических процессов. В качестве основного режима работы PLC выступает его длительное автономное использование, иногда в неблагоприятных условиях окружающей среды, без обслуживания и практически без вмешательства человека.

Рассмотрим сценарий атаки, EPC-модель которой представлена на рис. 5.

Злоумышленник, просканировав сеть, определил наличие в ней устройств, используемых в промышленной автоматизации – PLC. Определив модель PLC, он произвел поиск уязвимостей на PLC и обнаружил открытую уязвимость CVE-2018-4850. Воспользовавшись ей, злоумышленник перевел PLC в режим DEFECT после чего, PLC остается в этом режиме, пока он не будет перезапущен вручную.

Компания Siemens сообщила об обнаружении в ряде программируемых логических контроллеров SIMATIC S7-400 серьезной уязвимости CVE-2018-4850, позволяющей добиться отказа в обслуживании [11].

SIMATIC S7-400 представляет собой семейство программируемых логических контроллеров (ПЛК, PLC), предназначенных для управления технологическими процессами в промышленности. Продукт используется во всем мире в области автомобилестроения, производства механического оборудования, строительства, производства стали, производства и распределения электроэнергии, химического, складского, пищевого и фармацевтического секторов.

По словам представителей Siemens, данные устройства не проводят корректную проверку пакетов S7, позволяя удаленному злоумышленнику добиться отказа в обслуживании, заставив систему войти в режим DEFECT и оставаться в нем, пока она не будет перезапущена вручную.

Из сообщения Siemens следует, что для успешной эксплуатации злоумышленнику требуется отправить специально сформированный коммуникационный пакет S7 на коммуникационный интерфейс центрального процессора. В частности, речь идет об интерфейсах Ethernet, PROFIBUS и Multi Point Interfaces (MPI). В том числе, для эксплуатации уязвимости не требуется взаимодействие с пользователем или наличие каких-либо привилегий. [11, 12]

В настоящее время не зафиксировано случаев эксплуатации данной уязвимости киберпреступниками. Проблема затрагивает процессоры S7-400 с версией аппаратного обеспечения (АО) 4.0 и более ранними, процессоры S7-400 с версиями АО от 5.0 до 5.2, а также процессоры S7-400H с версиями АО 4.5 и более ранними. Для исправления уязвимости пользователям рекомендуется обновить версии аппаратного обеспечения до 5.0, 5.2 и 6.0 соответственно [11].

У современных PLC существует немалое количество различного рода уязвимостей, вот пример самых ярких из них: CVE-2014-2246, CVE-2014-2247, CVE-2014-2248, CVE-2014-2249, CVE-2014-2250, CVE-2014-2251, CVE-2014-2252, CVE-2014-2253, CVE-2017-7899. Остальные известные на сегодняшний день уязвимости можно просмотреть в National Vulnerability Database [13].

С развитием современных технологий и их широким распространением в системах автоматизации управления промышленного производства появляются все новые и новые уязвимости в программных и программно-аппаратных комплексах различных производителей. Зачастую многие уязвимости не учитываются разработчиками систем автоматизации на стадии производства из-за их неявного наличия (например, уязвимости нулевого дня). В большинстве случаев они обнаруживаются на этапах эксплуатации этих комплексов непосредственно в системах автоматизированного управления производством на промышленных предприятиях заказчиков после реализации атак злоумышленниками

либо в ходе аудита информационной безопасности специалистами самого промышленного предприятия. Все указанные уязвимости могут быть использованы для реализации атак в работающих АСУ ТП.

Как отмечено в работах [14–15] моделирование угроз является единственным способом тщательного изучения потенциальных деструктивных воздействий на информационную среду АСУ ТП.

Заключение

EPC модели угроз нарушения информационной безопасности позволяют оценить причинно-следственные связи между возможными уязвимостями АСУ ТП и негативными последствиями от их эксплуатации для безопасности системы промышленного предприятия. В данной работе представлены разработанные в ходе исследований EPC-модели угроз нарушения информационной безопасности основных компонентов АСУ ТП, такие как: модель угрозы замены на АРМ оператора программ управления PLC, угрозы нарушения информационной безопасности SCADA-сервера, угроза нарушения информационной безопасности OPC-сервера и PLC. Все перечисленные выше и описанные в работе угрозы исходят со стороны злоумышленника, находящегося за периметром КИС промышленного предприятия. Все угрозы также могут исходить и от внутренних нарушителей, являющихся сотрудниками промышленного предприятия, их следует принимать во внимание в ходе разработки комплекса технических и организационных мер для обеспечения необходимого уровня ИБ АСУ ТП. Построенные модели угроз позволяют проследить причинно-следственные связи между существующими уязвимостями компонентов АСУ ТП и последствиями для системы в контексте безопасности при реализации угроз.

СПИСОК ЛИТЕРАТУРЫ:

1. Гусев Н.В., Ляпушкин С.В., Коваленко М.В. Автоматизация технологических комплексов и систем в промышленности: учебное пособие / Томск: Изд-во Томского политехнического университета, 2011. – 198 с.
2. Воронцов А.Н., Автоматизированные системы управления технологическими процессами // Вопросы безопасности: информационный бюллетень компании “Инфосистемы Джет”. Информационная безопасность промышленных объектов. URL: http://www.jetinfo.ru/stati/asu-tp-voprosy-bezopasnosti (дата обращения: 06.01.2019).
3. Лукацкий А. Стандарты безопасности АСУ ТП // Cisco Systems, Москва, 2012. С. 5–15. URL: http://www.slideshare.net/ CiscoRu/ss-8690963 (дата обращения: 06. 01.2019).
4. Приказ ФСТЭК России от 14 марта 2014 г. №31. URL: http://fstec.ru/normotvorcheskaya/akty/53-prikazy/868-prikaz-fstek-rossii-ot/ (дата обращения: 06. 01.2019).
5. Что такое ERP система. Блог компании Trinion. URL: https://habr.com/company/trinion/blog/333018/ (дата обращения: 06.01.2019).
6. Система управления MES. Сайт Корпорации Галактика. URL: https://www.galaktika.ru/blog/mes.html (дата обращения: 06.01.2019).
7. Загидуллин Р.Р. Управление машиностроительным производством с помощью систем MES, APS, ERP. Старый Оскол: ТНТ. 2011. – 372 с.
8. Машкина И.В. Управление информационной безопасностью на основе интеллектуальных технологий: учебное пособие. Уфа: РИК УГАТУ. 2017. – 209 с. ISBN 978-5-4221-1087-2.
9. Шеер А.В. ARIS – моделирование бизнес-процессов. –М:. Вильямс, 2000. – 175 с.
10. CVE-2014-8551 Detail. URL: https://nvd.nist.gov/vuln/detail/ CVE-2014-8551 (дата обращения: 06.01.2019).
11. В ПЛК Siemens SIMATIC S7-400 обнаружена серьезная уязвимость. URL: https://www.securitylab.ru/news/493312.php (дата обращения: 06.01.2019).
12. Vulnerability Details: CVE-2018-4850. URL: https://www.cvedetails.com/cve/CVE-2018-4850/ (дата обращения: 06.01.2019).
13. National Vulnerability Database. URL: https://nvd.nist.gov/ (дата обращения: 06.01.2019).

14. Mashkina I., Garipov I., Development of Protection Object Model – Industrial Control System Using System Analysis. URL: https://ieeexplore.ieee.org/document/8501733 (дата обращения: 06.01.2019).
15. Mashkina I., Garipov I., Threats Modeling and Quantitative Risk Analysis in Industrial Control Systems. URL: https://ieeexplore.ieee.org/document/8501694 (дата обращения: 06.01.2019).

REFERENCES:

[1] Gusev N.V., Ljapushkin S.V., Kovalenko M.V. Avtomatizacija tehnologicheskih kompleksov i sistem v promyshlennosti: uchebnoe posobie Tomskij politehnicheskij universitet. [Automation of technological complexes and systems in industry: textbook Tomsk Polytechnic University.] Izdatelstvo Tomskogo politehnicheskogo universiteta, 2011. – 198 s. (in Russian).
[2] Voroncov A.N., Avtomatizirovannye sistemy upravlenija tehnologicheskimi processami. Voprosy bezopasnosti: informacionnaja bjulleten' kompanii “Infosistemy Dzhet”. [Automated control systems of technological processes the safety Issues: newsletter of the company “infosistemy Dzhet”] Informacionnaja bezopasnost' promyshlennyh ob#ektov. URL: http://www.jetinfo.ru/stati/asu-tp-voprosy-bezopasnosti (accessed: 06. 01.2019) (in Russian).
[3] Lukackij A. Standarty bezopasnosti ASU TP // Cisco Systems, [ICS safety standards. Cisco Systems] Moskva, 2012. S. 5–15. URL: http://www.slideshare.net/CiscoRu/ss-8690963 (accessed: 06. 01.2019) (in Russian).
[4] Prikaz FSTJeK Rossii ot 14 marta 2014 g. N 31. [Order fstec of Russia №31 of March 14, 2014] USB: http://fstec.ru/normotvorcheskaya/akty/53-prikazy/868-prikaz-fstek-rossii-ot/ (accessed: 06. 01.2019) (in Russian).
[5] Chto takoe ERP sistema. [What is ERP system] Blog kompanii Trinion. Data publikacii 14.07.2017. URL: https://habr.com/company/trinion/blog/333018/ (accessed: 06.01.2019) (in Russian).
[6] Sistema upravlenija MES. [MES control system] Sajt Korporacii Galaktika. URL: https://www.galaktika.ru/blog/mes.html (accessed: 06. 01.2019) (in Russian).
[7] Zagidullin R.R. Upravlenie mashinostroitel'nym proizvodstvom s pomoshh'ju sistem MES, APS, ERP. [Machine-building production management using MES, APS, ERP systems] Staryj Oskol: TNT. 2011. – 372 s. (in Russian)
[8] Mashkina I.V. Upravlenie informacionnoj bezopasnost'ju na osnove intellektual'nyh tehnologij: uchebnoe posobie. [Information security management based on intelligent technologies: tutorial] RIK UGATU. 2017. – 209 s. (in Russian).
[9] Sheer A.V. ARIS – modelirovanie biznes-processov. Vil'jams, Moskva, 2000. – 175 s. (in Russian).
[10] CVE-2014-8551 Detail. URL: https://nvd.nist.gov/vuln/detail/CVE-2014-8551 (accessed: 06. 01.2019).
[11] V PLK Siemens SIMATIC S7-400 obnaruzhena ser'eznaja ujazvimost'. [A serious vulnerability has been found in the Siemens SIMATIC S7-400 PLC] URL: https://www.securitylab.ru/news/493312.php (accessed: 06. 01.2019) (in Russian).
[12] Vulnerability Details: CVE-2018-4850. URL: https://www.cvedetails.com/cve/CVE-2018-4850/ (accessed: 06. 01.2019).
[13] National Vulnerability Database. URL: https://nvd.nist.gov/ (accessed: 06. 01.2019).
[14] Mashkina I., Garipov I., Development of Protection Object Model – Industrial Control System Using System Analysis. URL: https://ieeexplore.ieee.org/document/8501733 (accessed: 06. 01.2019).
[15] Mashkina I., Garipov I., Threats Modeling and Quantitative Risk Analysis in Industrial Control Systems. URL: https://ieeexplore.ieee.org/document/8501694 (accessed: 06. 01.2019).

Поступила в редакцию – 19 января 2019 г. Окончательный вариант – 7 ноября 2019 г
Received – January 19, 2019. The final version – November 7, 2019.