Д. Н. Любушкина, А. А. Оленников
Тюменский государственный университет, г. Тюмень
УДК 004.056.2, 004.056.53

АЛГОРИТМ ПРОВЕРКИ ПОДЛИННОСТИ ИСПОЛНИТЕЛЬНЫХ УСТРОЙСТВ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМ ПРОЦЕССОМ

Аннотация. В работе предложен алгоритм проверки подлинности исполнительных устройств АСУ ТП, основанный на стандарте HART, который может выступать как основная либо дополнительная мера защиты от угроз нарушения целостности системы. Рассмотрен принцип работы стандарта HART, приведен теоретический алгоритм, рассмотрены дополнительные технические решения, повышающие его надежность, а также сценарии возможных атак.

Ключевые слова: угрозы безопасности информации, АСУ ТП, целостность, стандарт HART.

Введение. АСУ ТП как один из типов ИС имеет ряд важных особенностей, среди которых — трехуровневая структура с различным набором протоколов и оборудования для каждого уровня, более серьезные и разрушительные потенциальные последствия от реализации угроз, актуальность угроз нарушения именно целостности и доступности [1]. Поскольку непосредственное взаимодействие АСУ ТП с физико-химическими, производственными процессами происходит на нижнем уровне — уровне исполнительных устройств — то вывод их из строя либо подмена с целью нарушения технологического процесса могут повлечь за собой серьезные происшествия.

Вопросы, касающиеся проблем ИБ АСУ ТП, рассматриваются в немалом количестве работ. Так, в статье «Проблемы информационной безопасности АСУ ТП» за авторством студентов Уральского федерального университета верно отмечено, что «современные АСУ ТП подвержены разнообразным угрозам со стороны внутренних и внешних злоумышленников (террористические, экстремистские и враждебно настроенные группы) с целью вывести системы из строя», однако спорным является утверждение: «…мало кому будут

полезны и интересны данные с датчиков», поскольку от корректности этих данных напрямую зависит целостность, непрерывность и безопасность технологического процесса, также такие данные могут быть интересны конкурирующим организациям, например, если технологический процесс предполагает какие-либо секретные либо экспериментальные разработки [2].

Обзор других исследований по теме показал, что основными методами обеспечения ИБ АСУ ТП являются, помимо правовых, технические меры, работающие на верхнем уровне сетевой инфраструктуры: управление трафиком, его ограничение, журналы событий, физическое ограничение доступа к промышленному сегменту и так далее, а также организационные, например, регламентирование уровней допуска и так далее [3-6]. Безусловно, эти методы повышают уровень защищенности, но не могут в полной мере защитить от угроз, реализуемых, например, при физическом доступе в сеть.

Проблема исследования. Существующие решения, представленные различными программно-аппаратными комплексами, могут быть нецелесообразны для небольших систем с низким классом защищенности и (или) не относящихся к объектам КИИ в силу большой стоимости и избыточности функционала. В ходе их изучения были сформулированы следующие проблемы:

- отсутствие аутентификации и шифрования у промышленных протоколов — присутствует только контроль целостности данных обеспечивается контрольными суммами [7];
- сосредоточение существующих решений преимущественно на обеспечении защищенного канала между верхним и средним уровнями АСУ ТП, в то время как безопасность взаимодействия нижнего и среднего уровней реализована в основном за счет физических ограничений;
- контроль целостности исполнительных устройств преимущественно по наблюдению за отклонением от уставок технологического процесса.

Алгоритм, предлагаемый в статье, является попыткой организации защищенного канала между нижним и средним уровнями сети АСУ ТП.

Материалы и методы. Реализация основана на возможностях стандарта HART [8-12]. Это популярный стандарт связи в промышленности, в котором данные передаются посредством комбинирования цифрового сигнала, с которым передается информация об оборудовании, и аналогового, с которым передаются измерения. HART-устройства всегда содержат микроконтроллер, в числе компонентов которого имеется ППЗУ, где содержится вся информация об устройстве. У HART-устройства есть уникальный идентификатор, состоящий из ID-изготовителя, кода типа устройства и серийного номера. Этот идентификатор, ввиду сложности его подмены, можно использовать для проверки подлинности.

Блок-схема обобщенного алгоритма самодиагностики устройств с возможностями использования HART-стандарта и дополнительным контролем за соблюдением уставок представлен на рис. 1.

Недостаток промышленных протоколов — отсутствие шифрования — возможно компенсировать штатными средствами. Так, передаваемые ключи контроля целостности должны передаваться с ПЛК уже в зашифрованном виде, а исполняемую программу ПЛК и задействованные криптографические библиотеки следует как минимум защитить сложным паролем (такая возможность есть во многих IDE) от чтения/записи. Некоторые ПЛК имеют поддержку шифрования аппаратными ключами и физические ключи-перемычки для ограничения функциональности в режиме эксплуатации, что стоит использовать, если есть возможность.

Результаты. Разработанный алгоритм является концепцией средства безопасности канала связи между нижним и средним уровнями сети АСУ ТП и основан на возможностях физических протоколов. Как и любой алгоритм безопасности, необходимо рассмотреть возможные пути обхода и актуальных нарушителей.

В качестве злоумышленника для обозначенных систем могут выступать внутренний и внешний нарушители с низким потенциалом (H1, H2), описание возможностей которых соответствует таблице 8.1 из «Методики оценки угроз безопасности информации» [10]. Иллюстрация к сценариям представлена на рис. 2.

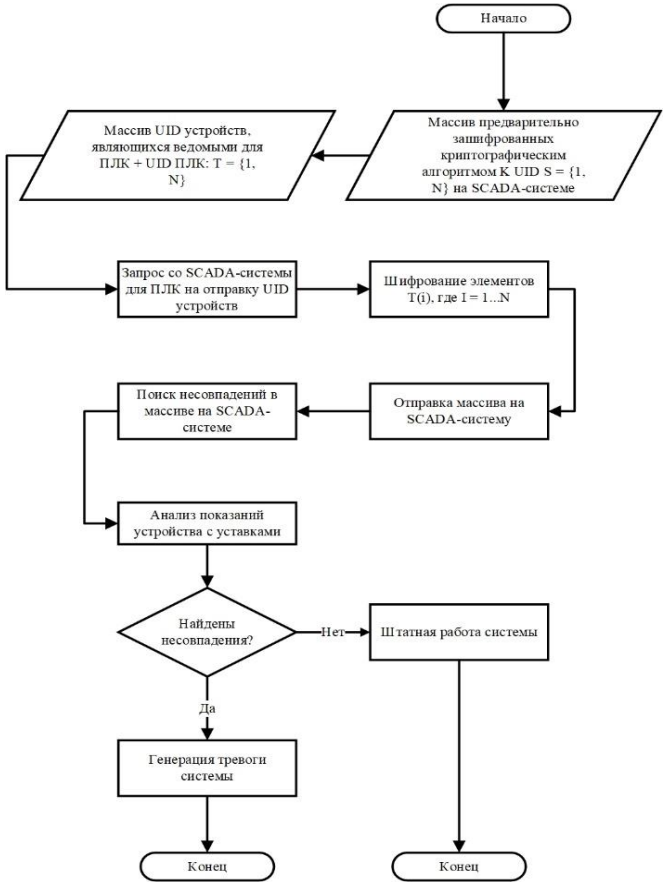

Рис. 1. Блок-схема алгоритма

Сценарий 1: нарушитель получает удаленный доступ к SCADA-системе. Первый вариант: нарушитель получает доступ к файлам программы ПЛК, например, из хранилища резервных копий; тогда злоумышленнику необходимо обойти защиту программы, но нельзя определить наверняка, что программа актуальна и в ней содержатся необходимые библиотеки. Второй вариант: нарушитель получает доступ к передаваемым на SCADA-систему тегам; в таком случае,

поскольку необходимые для проверки теги передаются уже зашифрованными, злоумышленнику придется решать сложную задачу дешифрования.

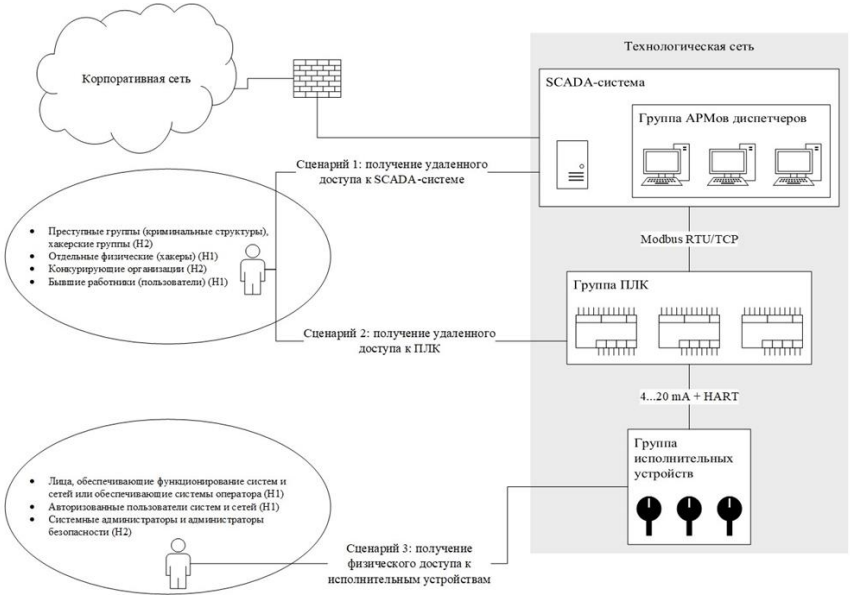

Рис. 2. Сценарии атак на алгоритм

Сценарий 2: нарушитель получает удаленный доступ к ПЛК. Поскольку одним из основных требований является ограничение доступа к исполняемой программе ПЛК методами, указанными выше, то нарушителю необходимо обойти как минимум шифрование паролем — причем различные компоненты программы могут быть зашифрованы разными паролями. Также программа может быть недоступна для чтения из-за физических ограничений. Без доступа к исполняемой программе ПЛК злоумышленник никаким образом не сможет получить удаленный доступ к сегменту технологической сети, находящийся за ПЛК.

Сценарий 3: нарушитель получает физический доступ в КЗ. В таком случае, недостаточно просто подменить устройства. В первом

варианте развития событий нарушителю необходимо получить доступ к SCADA-системе и исполняемой программе ПЛК с целью подмены сведений об устройствах, а также успеть квитировать сигналы аварии, которые получит SCADA-система вследствие отключения устройства, до того, как система оповестит дежурный персонал; сценарий требует организованной группы лиц. Во втором варианте злоумышленник может попытаться получить доступ к микроконтроллерному обеспечению устройства и модифицировать его; для этого требуется высокий уровень подготовки в электросхемотехнике и радиоэлектронике, что также, вероятно, недоступно для нарушителя с потенциалом Н1, Н2, и не является достаточно эффективным способом реализации атаки. В третьем варианте нарушитель перехватывает данные непосредственно от датчиков при помощи дополнительного оборудования и получает ключи проверки подлинности или может подменить передаваемое датчиком значение; в этой ситуации среагирует SCADA-система, которая должна выдавать аварии и предупреждения при отклонении показаний на основании заданных уставок, а также проводить проверку корректности значений.

Заключение. В работе предложено возможное решение для защиты канала передачи данных между нижним и средним уровнями сети в АСУ ТП, основанное на использовании не только контроля по уставкам, но и возможностей физических протоколов связи. Рассмотрены сценарии атак на алгоритм. Такой алгоритм может стать альтернативным решением для небольших АСУ ТП, не относящихся к числу объектов КИИ и имеющих низкий КЗ, для которых может быть экономически нецелесообразно использовать отдельные комплексные решения, поскольку алгоритм задействует штатные средства программирования ПЛК и возможности датчиков с поддержкой стандарта HART. Дальнейший вектор развития идеи — создание устройства безопасности, которое сможет шифровать данные сразу на выходе датчика, обрабатывая суммированный HART-сигнал — это позволило бы свести к минимуму вероятность реализации сценария атаки, где злоумышленник смог получить физический доступ к промышленной сети.

СПИСОК ЛИТЕРАТУРЫ

1. 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: Приказ № 31: утвержден ФСТЭК России 14.03.2014. — Москва, 2014. — 31 с. — Текст : непосредственный.
2. Вольхина М.Н. Проблемы информационной безопасности в АСУ ТП / М.Н. Вольхина, К.Л. Стойчин // Безопасность информационного пространства — 2017: XVI Всероссийская научно-практическая конференция студентов, аспирантов, молодых ученых. Екатеринбург, 12 декабря 2017 года. — Екатеринбург: Изд-во Урал. ун-та, 2018. — С. 96-99.
3. Пищик Б.Н. Безопасность АСУ ТП / Б. Н. Пищик // Вычислительные технологии. — 2013. — Т. 18. — Специальный выпуск 1: Труды Всероссийской конференции «Индустриальные информационные системы-2013» на русском и английском языке — С. 170-175.
4. Анализ рисков безопасности автоматизированных систем управления технологическими процессами / Г.П. Цапко, А.А. Вериго, А.С. Каташев // Интернет-журнал «НАУКОВЕДЕНИЕ». — 2016. — Т. 8, № 5. — С. 1-9.
5. Особенности обеспечения информационной безопасности промышленных систем автоматизации в соответствии с приказом ФСТЭК № 31 / А. Табульда, С. Чернущенко // СТА. — 2016. — № 4. — С. 100-104.
6. Современные подходы к обеспечению информационной безопасности автоматизированных систем управления технологическими процессами / А. Ю. Кравчук, Н. А. Котова, И. И. Аничкин // Инновации и инвестиции. — 2022. — №3. — С. 191-195.
7. Modbus messaging on tcp/ip implementation guide v1.0b : [сайт]. — URL: https://modbus.org/docs/Modbus_Messaging_Implementation_Guide_V1_0b.pdf. — Текст: электронный.
8. Application of the hart protocol for communication with smart field devices / Mulaosmanovic Adnan M // Military technical courier. — 2015. — Vol. 63, № 3. — Pp. 160-175.
9. HART протокол: общие сведения и принципы построения сетей на его основе / В. Денисенко // СТА. — 2010. — № 3. — С. 94-101.
10. HART-протокол / В. Половинкин // СТА. — 2002. — № 1. — С. 6-14.

11. HART-IP® Application, Communication, and Control Analysis: [сайт]. — URL: https://www.fieldcommgroup.org/sites/default/files/imce_files/technology/documents/HART_IP_%20Application_Communication_Analysis_r1.0.pdf — Текст: электронный.
12. Анализ целесообразности использования HART протокола при создании и модернизации АСУ ТП энергометаллургического комплекса / С. Г. Супрунов, В. Г. Лисиенко // Теплотехника и информатика в образовании, науке и производстве: сборник докладов IV Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых «Теплотехника и информатика в образовании, науке и производстве» (ТИМ'2015) с международным участием, посвященной 95-летию основания кафедры и университета (г. Екатеринбург, 26-27 марта 2015 г.). — Екатеринбург: УрФУ, 2015. — С. 408-411.
13. Методический документ. Методика оценки угроз безопасности информации: утвержден ФСТЭК России 05.02.2021: [сайт]. — URL: https://www.consultant.ru/document/cons_doc_LAW_378330/. — Текст: электронный.