УДК 004.056

Д.Б. Жмуров

Россия, Самара, Самарский национальный исследовательский университет имени академика С.П. Королева

АНАЛИЗ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ

Анализируются существующие подходы к анализу векторов угроз безопасности информации в АСУТП. Формулируется и обосновывается тезис о том, что большинство декларируемых угроз АСУТП относятся к автоматизированным системам в целом, а не только к АСУТП. Приводятся вектора угроз, существующих на полевом уровне АСУТП, которые в последующем могут лечь в основу разработки соответствующих методов и средств защиты.

Ключевые слова: угрозы безопасности, АСУТП, ПЛК, полевой уровень АСУ, Modbus.

Введение

За последнее время на специализированных информационных ресурсах всё чаще затрагиваются вопросы информационной безопасности автоматизированных систем управления технологическими процессами (АСУТП). Средства массовой информации, аудиторские компании публикуют данные о росте количества хакерских атак на промышленные предприятия, повлекшие за собой остановку производства, поломку оборудования и другие материальные потери.

Разработчики программно-аппаратных комплексов продвигают на рынок новые решения, предназначенные для защиты вычислительных сетей промышленных предприятий и АСУТП.

Однако в рядах специалистов по АСУТП существует мнение, что рассмотрение проблем информационной безопасности АСУТП проводится без учета специфики самих АСУТП, при этом специфика АСУТП плохо учитывается при построении модели угроз АСУТП.

Целью данной работы является попытка обозначить слабые места в предлагаемых на сегодняшний день подходах по информационной безопасности

АСУТП и обозначить проблемы, специфичные именно для АСУТП, т.е. не встречающиеся в других автоматизированных системах.

1. Существующий подход к построению защищенной АСУТП

В 2016 году специалистами ведущего отечественного производителя антивирусного ПО «Лаборатория Касперского» опубликованы аналитические обзоры, посвященные анализу уязвимостей промышленных систем автоматизации [1 и др.]. В указанных материалах приводится анализ уязвимостей ПО, используемого на АРМ промышленных предприятий, угроз вирусных программ и таргетированных кибератак. Аналогичный материал можно найти на других специализированных ресурсах и блогах специалистов по ИБ [2 и др.].

Наиболее кратко и наглядно виды и направления угроз иллюстрируются на рисунке из отчета специалистов «Лаборатории Касперского» [1], представленного на рисунке 1.

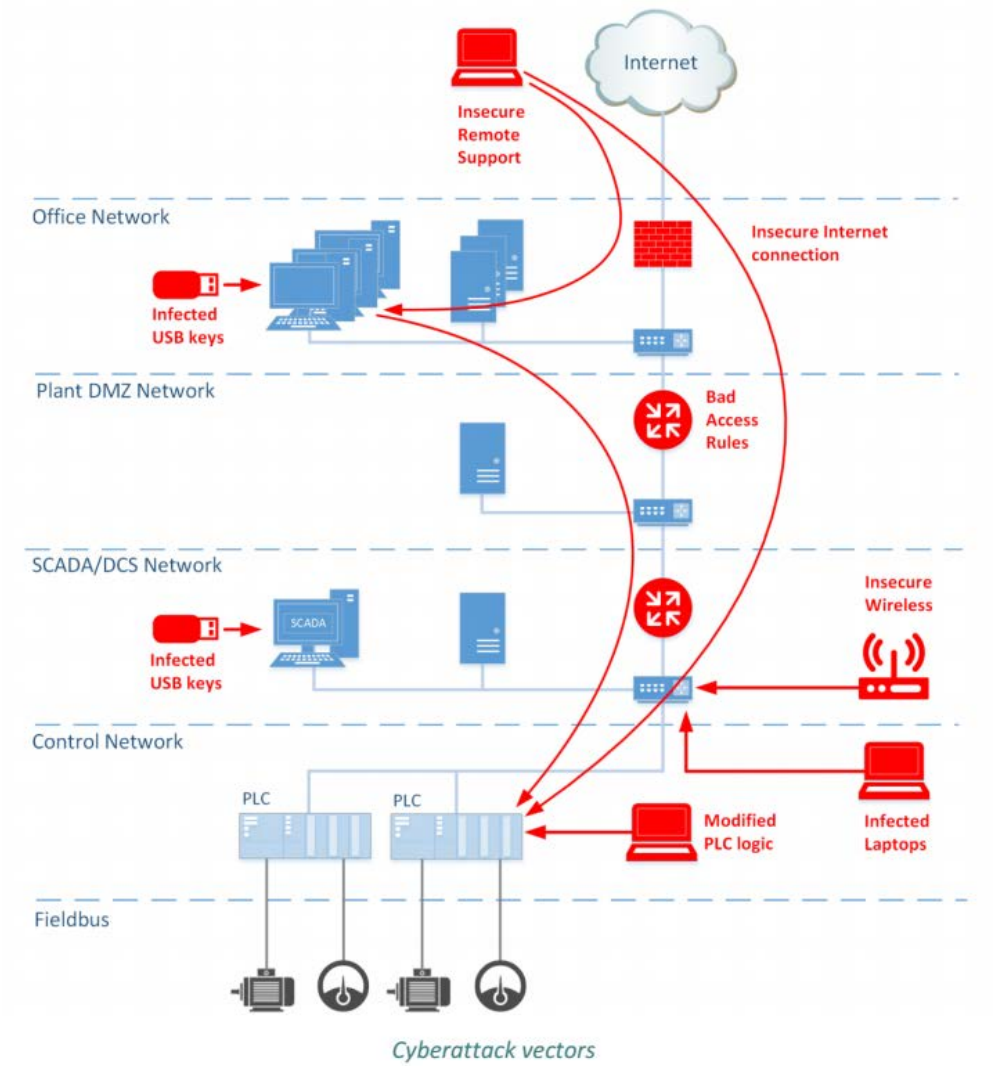

Рисунок 1 – Модель угроз информационной безопасности АСУТП

Таким образом, предлагается рассматривать следующие векторы атаки:

1) незащищенный каналтехнической поддержки (InsecureRemoteSupport);

2) незащищенное интернет-соединение (InsecureInternetConnection);

3) зараженные отчуждаемые носители (InfectedUSBKeys);

4) неправильные правила доступа в межсетевых шлюзах (BadAccessRules);

5) незащищенное беспроводное соединение;

6) зараженные подключаемые переносные компьютеры (InfectedLaptops);

7) модификация программы для ПЛК (ModifiedPLCLogic).

2. Критический анализ существующей моделиугроз

Общий взгляд на представленную модель позволяет сделать вывод, что перечисленные угрозы эксплуатируют искусственно созданные уязвимости (которых не должно быть при правильном проектировании системы) или не относятся проблеме защиты именно АСУТП. Рассмотрим перечисленные выше уязвимости подробнее.

2.1. Незащищенный канал технической поддержки

Данный вид угроз, очевидно, заимствован из модели защиты автоматизированных систем обработки информации и управления (АСОИУ), где удаленная техническая поддержка и обслуживание систем является обычным делом и широко распространена.

Однако удаленная техническая поддержка в АСУТП является лишним звеном по перечисленным ниже причинам.

1. Управление технологическими процессами осуществляется по жестко заданным алгоритмам, множество состояний процесса предопределено и является конечным. Необходимость внесения изменений в алгоритмы работы является следствием пробелов при разработке и пуско-наладке АСУТП и не относится к проблематике информационной безопасности.

2. Модернизация алгоритмов и компонентов АСУТП, при необходимости, проводится во время плановой остановки производства. В этом случае наиболее эффективно личное присутствие профильных специалистов по АСУТП для подготовки и запуска производства.

3. Противодействие внезапным сбоям и отказам оборудования решается применением специальных технических решений, выполняющих горячее резервирование важных компонентов АСУТП (например, резервированные ПЛК Siemensлинеек S300 и S400).

2.2. Модификация программы для ПЛК

Реализация данной угрозы может приводить к существенным убыткам, однако, как показано на рисунке 1, данное событие возможно при наличии физического доступа к оборудованию.

Следует отметить, что ПЛК всегда находится внутри охраняемой зоны, зачастую за вторым или третьим периметром инженерно-технической защиты. Поэтому реализация данной угрозы возможна в двух случаях: в результате проникновения злоумышленника в охраняемый периметр или действия персонала предприятия.

В первом случае данная угроза не является специфичной для обеспечения ИБ АСУТП, поскольку является пробелом в организации режима охраны предприятия.

Во втором случае данная угроза является следствием недочётов в обеспечении трудовой дисциплины. Очевидно, что трудовая дисциплина является обязательной на любом предприятии, не зависимо от наличия АСУТП, поэтому в этом случае угроза неспецифична АСУТП.

2.3. Прочие виды угроз

Оставшиеся виды угроз, показанные на рис.1, относятся к проблематике построения защищенных вычислительных сетей и контроля оборота отчуждаемых носителей.

В частности, грубой ошибкой является объединение промышленной и офисной сетей. Использование беспроводного канала связи на производстве является не только нецелесообразным, но и может оказаться малоэффективным вследствие зашумленности используемого диапазона частот.

В целом, методы противодействия обозначенным угрозам уже достаточно подробно исследованы и отражены в соответствующих нормативных документах и не являются специфичными применительно к защите АСУТП.

3. Выделение специфических угроз безопасности АСУТП

В предыдущих пунктах было показано, что описываемые угрозы не специфичны для АСУТП и применимы для большинства автоматизированных систем различного назначения.

Это объясняется тем, что они направлены на уровень автоматизированной системы управления производством (АСУП), который располагается выше уровня АСУТП. Согласно п.7 приказа ФСТЭК России №31 от 14.03.2014 [4] к АСУТП относятся уровниотSCADANetworki ниже.

Теперь рассмотрим угрозы, наиболее актуальные для АСУТП и отсутствующие в представленной модели угроз.

3.1. Недекларированные возможности программы ПЛК

Руководящие документы [3-4] регламентируют контроль недекларированных возможностей (НДВ) в средствах защиты информации. Как правило, ПЛК имеют средства защиты от несанкционированного подключения остановки и модификации программы управления технологическим процессом. Однако более важно контролировать НДВ в логике управления.

Использование НДВ в логике управления позволяет атаки на производство, например внезапные остановки, как с целью нанести материальный вред, так и с целью получения денег за платный «ремонт».Следует отметить, что в данном случае бессильны средства ПАЗ, поскольку они также в этом случае содержат НДВ в логике работы.

3.2. Физические интерфейсы и протоколы полевого уровня

Передаваемые на полевом уровне данные не являются конфиденциальными. Атака на их доступность обычно не являются критичными, поскольку разработчики АСУТП предусматривают безопасные режимы работы при отказе каналов связи с периферийным оборудованием.

Наиболее опасной уязвимостью является подмена технологических данных, таких как измеренные значения физических величин, состояния исполнительных механизмов и т.п.

На сегодняшний день широкое распространение имеет протокол Modbus, работающий по шине RS485, а также аналогичные проприетарные протоколы ведущих производителей (Owenbus, Toshibabusи др.).

Работающие по указанным протоколам устройства не используют механизмов идентификации и аутентификации. Это дает возможность подмены как ведущего устройства (мастера шины) с выдачей вредоносных команд (слов управления) ведомым устройствам, так и ведомых устройств с выдачей поддельных данных состояния (слов состояния). Причем каналы связи могут проходить за пределами контролируемой зоны, а также малодоступных для контроля местах, что упрощает несанкционированное подключение.

Традиционным способом защиты автоматизированных систем от указанных угроз является использование брандмауэров. Однако их применение на полевом уровне сопряжено с рядом трудностей:

– введение дополнительного устройства в канал передачи данных снижает его скорость, что может быть критичным для качества управления технологическим процессом, а также снижает надежность канала;

– для объектов управления чувствительным параметром является размер шкафа автоматики, а дополнительные устройства занимают полезный объем;

– брандмауэры должны изготавливаться в промышленном исполнении, что существенно повышает их стоимость;

– на объекте управления может отсутствовать физическая возможность размещения и подключения брандмауэров.

Заключение

Таким образом, в настоящей работе показано, что декларируемые на сегодняшний день угрозы ИБ для АСУТП и методы противодействия им являются актуальными для АС вообще и не учитывают специфику АСУТП.

Также показано, что угрозы, существующие на полевом уровне АСУ изучены еще недостаточно, средства и методы ЗИ для полевого уровня еще не получили распространения.

Литература

1. Threat landscape for industrial automation systems in the second half of 2016 // https://ics-cert.kaspersky.com/reports/2017/03/28/threat-landscape-for-industrial-automation-systems-in-the-second-half-of-2016.

2. Артамонов В.А. Информационная безопасность систем управления критически важными объектами // ПРОЕКТ «ИТ-ЗАЩИТА» http://itzashita.ru/publications/informatsionnaya-bezopasnost-sistem-upravleniya-kriticheski-vazhnyimi-obektami-chast-3.html.

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

4. РД приказ председателя Гостехкомиссии России от 4 июня 1999 г. N 114 «Защита от несанкционированного доступа к информации. Часть 1.Программное обеспечение средств защиты информацииКлассификация по уровню контроля отсутствия недекларированных возможностей».