Analysis of the problems of information security of automated process control systems
Abdugulova J.[1], Mashtayeva A.[2] (Republic of Kazakhstan)

Анализ проблем информационной безопасности автоматизированных систем управления технологическими процессами
Абдугулова Ж. К.[1], Маштаева А. А.[2] (Республика Казахстан)

[1]Абдугулова Жанат Капаровна / Abdugulova Janat Kaparovna – кандидат экономических наук, доцент;
[2]Маштаева Аида Асильхановна / Mashtayeva Aida Asilkhanovna – студент,
кафедра системного анализа и управления,
факультет информационных технологий,
Евразийский национальный университет им. Л. Н. Гумилева, г. Астана, Республика Казахстан

Аннотация: *в статье приведен краткий обзор проблем информационной безопасности автоматизированных систем управления технологическими процессами.*
Abstract: *the article provides a brief overview of the problems of information security of automated process control systems.*

Ключевые слова: *автоматизированная система управления технологическим процессом (АСУ ТП), информационная безопасность (ИБ), программное обеспечение (ПО).*
Keywords: *automated process control systems, information security, software.*

Проблема безопасности АСУ ТП на промышленных предприятиях никогда не стояла так остро, как в последние несколько лет. Интерес к проблеме возник после инцидентов с вирусами, атаковавшими промышленные объекты. Ранее считалось, что в работу АСУ ТП довольно трудно вмешаться. Такое представление базировалось на нескольких постулатах: ПО каждой АСУ ТП уникально и закрыто; локальная сеть АСУ ТП решает проблемы ограничения доступа; проникновение в АСУ ТП связано с большими затратами, а вознаграждение не очевидно [1, с. 36]. Изучение структуры и программно-аппаратных средств показало, что за последнее время произошли существенные изменения. Повсеместно используется ПО, которое вместе со своими достоинствами принесло и недостатки. Специалисты по ИБ, исследовавшие код вируса, сделали вывод, что он предназначался для точечной атаки определённого производства или ряда производств. Согласно анализу, вредоносный код реализовывал атаку сразу на нескольких уровнях: на уровне операционных систем, ПО управления АСУ ТП и программируемых логических контроллеров (ПЛК). Обзор состояния безопасности АСУ ТП показал довольно тревожную картину. Увеличивается число обнаруженных уязвимостей. Каждая пятая уязвимость устраняется дольше месяца. Половина позволяют хакеру запустить выполнение кода. Основные проблемы ИБ АСУТП, выделяемые экспертами, проистекают: из слабой защиты от несанкционированного доступа (пароли); недекларированных возможностей SCADA; отсутствия контроля управляющих воздействий (совокупность параметров); использования беспроводных коммуникаций; отсутствия чётких границ между разными сегментами сети; несвоевременного или некорректного обновления ПО; дистанционных методов управления; Web-технологий, используемых в АСУ ТП; отказа даже от минимальных мер безопасности; человеческого фактора или слабой дисциплины сотрудников и т. д. Приведём перечень основных угроз АСУ ТП, отмеченных в реальных инцидентах: атаки на SCADA; атаки на PLC, уязвимости PLC; атаки на инфраструктуру и оперативную систему (вирусы); атаки на протоколы, уязвимость протоколов; атаки баз данных (несанкционированный доступ, SQL инъекция); практические атаки (переполнение буфера, отказ в доступе, управлении) [2, с. 271]. Вследствие длительности эксплуатации АСУ ТП и существенного изменения состава и качества современных угроз необходимо проектировать и реализовывать ИБ систем с учётом тенденций развития киберугроз. С другой стороны, необходимо проводить регулярную работу по нейтрализации возникающих или потенциальных угроз на работающих системах. Совокупность нейтрализующих мер можно разделить на две группы: административно-организационные и программно-технические. Первая группа мер связана с формированием программы работ по обеспечению ИБ АСУ ТП и разработкой набора документов, которые регламентируют высокоуровневый подход по обеспечению ИБ, а также описывают политику развития системы ИБ АСУ ТП. Программно-технические меры образуют основной набор средств обеспечения ИБ АСУ ТП. На этом уровне реализуются следующие сервисы ИБ: управление доступом, обеспечение целостности, обеспечение безопасного межсетевого взаимодействия, антивирусная защита, анализ защищённости, обнаружение вторжений, управление системой ИБ.

Литература

1. *Белогорцев Е. В.* Автоматизированные системы управления. М.: Электронная книга БГУ, 2004. 36 с.
2. *Пьявченко Т. А., Финаев В. И.* Автоматизированные информационно-управляющие системы. М.: Издательство ТРТУ, 2007. 271 с.