УДК 654.949

Курсант В.А. Амелин
Науч. рук. ст. преп. Д.Г. Назаров
(кафедра РЭТ ВВС и войск ПВО БГУИР, г. Минск)

СОВРЕМЕННЫЕ ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ В АСУ ТП

Под защитой информации в автоматизированных системах управления технологическим процессом (АСУ ТП) следует понимать комплекс практических взаимосвязанных мероприятий, направленных на предотвращение раскрытия, несанкционированного использования, изменения, искажения, уничтожения, копирования, шпионажа и прочих негативных вмешательств в АСУ ТП. Типичная АСУ ТП имеет от двух до трёх уровней сетевой архитектуры. На современных предприятиях все чаще реализуется единая среда управления в корпоративной сети в которой размещены компьютеры и системы, посредством которых осуществляется управление организационной и финансовой деятельностью. Часть компьютеров может иметь доступ к серверам АСУ ТП, содержащим накапливаемую о технологическом процессе информацию. Сеть АСУ ТП может иметь верхний уровень (станции операторов и инженеров АСУ ТП, серверы баз данных, серверы приложений), средний уровень (программируемые логические контроллеры) и нижний уровень (датчики сбора данных и исполнительные механизмы). Связь между уровнями обеспечивается коммуникационными серверами или контроллерами. Современной тенденцией является использование IP и Ethernet сетей на верхнем и среднем уровнях. Всё чаще промышленные устройства имеют Ethernet порты и IP протоколы, которые используются на всех уровнях сети АСУ ТП. Таким образом, особенностью сетей АСУ ТП является использование в дополнение к IP ещё и специализированных протоколов, которые если и затрудняют проникновение, то, как показывают инциденты, не для профессионалов. Следует отметить, что соединение по специальным протоколам, как правило, не предусматривает средств защиты. 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, троянские программы, черви, DDoS-атаки, ARP-спуфинг – перехват трафика после объявления себя маршрутизатором); – атаки на протоколы, уязвимость протоколов (OPC – переполнение буфера, нестойкий пароль); – атаки баз данных – практические атаки. Вследствие длительности эксплуатации АСУ ТП и существенного изменения состава и качества совре-

менных угроз необходимо проектировать и реализовывать информационную безопасность 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 информационной безопасности (ИБ) АСУ ТП и разработкой набора документов, которые регламентируют высокоуровневый подход по обеспечению ИБ, а также описывают политику развития системы ИБ АСУ ТП. Кроме того, формируется пакет организационной документации, направленной на создание и поддержание режима 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 Конкретные требования к перечисленным сервисам предъявляются на основании анализа обрабатываемой информации и оценки угроз безопасности АСУ ТП. Каждая группа мер в зависимости от необходимости и возможностей предприятия может осуществляться на одном из трёх уровней. Базовый уровень включает механизмы, традиционные для большинства информационных систем. Средний уровень предполагает выполнение начальных мероприятий, обеспечивающих реализацию управляемых защитных функций по обеспечению ИБ. На расширенном (высоком) уровне реализуются мероприятия, поддерживающие и расширяющие базовый и средний уровень, но для их реализации может потребоваться дополнительная экспертиза. Зона ЛВС АСУ ТП отделяет критичные системы АСУ ТП и состоит из нескольких функциональных зон. Нулевой уровень – датчики сбора данных и исполнительные механизмы. Первый уровень – узлы коммутации, обеспечивающие подключение датчиков к ПЛК. Второй-третий уровень – ПЛК, рабочие места операторов, серверы хранения данных. Могут использоваться межсетевые экраны и IDS. Демилитаризованная зона обеспечивает связность корпоративной ЛВС и ЛВС АСУ ТП. Она содержит только некритичные системы, которым необходим доступ к корпоративной ЛВС и ЛВС АСУ ТП, состоит из нескольких функциональных зон и отделена межсетевыми экранами и IPS. Однако перед научным сообществом поставлены серьѐзные задачи в области развития фундаментальной и прикладной науки, технологий и

средств обеспечения безопасности автоматизированных систем управления.

ЛИТЕРАТУРА

1. Обеспечение информационной безопасности АСУ ТП с использованием метода предиктивной защитыВопросы кибербезопасности. 2019. № 2.

2. Гарбук С. В., Гриняев С. Н., Правиков Д. Ю., Полянский А. В. Обеспечение информационной безопасности АСУ ТП с использованием метода предиктивной защиты Текст научной статьи по специальности «Компьютерные и информационные науки».

УДК 658.512

Курсант А.А. Кашко
Науч. рук. преп. Н.Н. Лавринчик
(кафедра РЭТ ВВС и войск ПВО БГУИР, г. Минск)

АВТОМАТИЗАЦИЯ ПРОИЗВОДСТВА

В условиях стремительно развивающихся технологий предприятиям необходимы новые решения, позволяющие:

- увеличивать объемы выпускаемой продукции;
- осуществлять трудоемкие технические задания за меньший промежуток времени;
- сокращать расходы сырья и отходов;
- выполнять недоступную человеческим рукам работу.

Решить данный ряд задач под силу только инновационным системам, таким, как автоматизация производства, т.е. передача управленческих и контрольных функций от человека к техническому оборудованию.

Основная роль внедрения систем автоматизации – повышение уровня эффективности, мобильности и облегчения труда сотрудников. Благодаря этим изменениям возрастает уровень конкурентоспособности на рынке, идет мощное использование ресурсной базы.

Автоматизация производства может быть осуществлена в нескольких вариантах.

1. Частичная. Автоматизации подвергается лишь некоторое оборудование, которое выполняет ряд действий, недоступных или сложных для человека.

2. Комплексная. Охватывает производственную цепь отдельного цеха или узла, выполняющего ряд действий по решению определенной задачи.