УДК 004.056.5:378.3

Особенности активного аудита информационной безопасности АСУ предприятия

Подтопельный Владислав Владимирович – старший преподаватель кафедры Информационной безопасности Балтийской государственной академии рыбопромыслового флота Калининградского технического университета.

Аннотация: Рассмотрены особенности активного аудита информационной безопасности систем обработки информации и управления. Указаны особенности анализа результатов активного аудита автоматизированных систем управления технологическими процессами. Приведены особенности фаз аудита многоуровневых информационных систем.

Ключевые слова: Сетевые атаки, сетевое правило, сигнатура, система обнаружения вторжений, угроза, протокол.

После введения в действие приказа ФСТЭК №31 от 14 марта 2014 г. возникла необходимость рассмотреть более подробно проблемную область аудита подсистем АСУ ТП[1]. Требуется определить особенности поиска уязвимостей в автоматизированных системах управления с учетом специфики технологических процессов, а так же особенности методики анализа сочетания угроз и уязвимостей.

Пассивный аудит позволяет решать вопросы анализа состояния безопасности систем без взаимодействия с системными элементами, в то время как аудит активного типа при работе с компонентами АСУТП сильно ограничен. Трудность состоит в том, что компоненты автоматизированных систем управления, размещенные на разных уровнях, сильно различаются по технологии исполнения. Ограничения, прежде всего, связаны с технологиями, которые реализуются на уровнях компонентов обрабатывающих техническую информацию от полевых устройств. При этом другие уровни АСУ с данной информации уже не работают. Данные особенности следует учесть при определении способов анализа угроз и уязвимостей.

Кроме того, аудит активного типа при взаимодействии с компонентами АСУТП не должен нарушить технологию обработки данных и при этом в результате тестирования должен быть получен максимум информации о состоянии системы. Также и сама методика анализа результатов должна учитывать указанные особенности аудита активного типа. Следовательно, необходимо найти такую методику анализа безопасности подсистем АСУ ТП, которая бы учитывала, с одной стороны, уровневую архитектуру системы, а, с другой стороны, технические особенности, как функционирования подсистем, так и процедур аудита[2].

При определении специфики тестирования выделяют следующие уровни АСУ: уровень планирования, уровень управления, уровень диспетчерского управления, уровень автоматического управления, полевой уровень. Предполагается, что каждый из этих уровней уязвим. Однако сами уязвимости различаются в соответствии с различиями применяемых на уровне АСУ технологий. Следует отметить, что на уровнях, расположенных над диспетчерским слоем, скорость передаваемой информации не критична так, как на полевом или диспетчерском уровне, поскольку компоненты этих (нижних) уровней транслируют данные по сети в режиме реального времени (с минимальной задержкой, при этом большие задержки по времени передачи не допустимы) [3]. Соответственно, время задержки в этом случае является показателем критичности.

Следуя требованию учитывать технологии уровней АСУ при тестировании, можно сделать вывод о том, что аудит будет заключаться в отдельном исследовании и анализе каждого технологически отличного уровня. И только после полного исследования состояния всех уровней, суммируя полученные данные, можно будет оценить общую уязвимость или защищенность системы.

При анализе результатов активного аудита удобно применять граф компрометации, который учитывает вероятностные показатели проникновения в систему с учетом всех ситуаций, которого могут возникнуть у злоумышленника, а также с учетом времени, которое затрачивает злоумышленник для достижения заданных им целей. Основным показателем уровня защищенности/незащищенности является время, затрачиваемое злоумышленником на достижения целей компрометации на каждом слое. При этом, чем больше время, затрачиваемое на компрометацию, тем выше вероятность отражения атаки. Таким образом, время компрометации каждого слоя АСУ, учитывая все действия атакующего, определяются по формуле[4]: