

УДК 621.3

### Технические решения по защите АСУ ТП АЭС от кибератак

Федосевич Э. А.

Научный руководитель – САПОЖНИКОВА А. Г.

Все защитные меры могут быть разделены на 5 блоков, каждый из которых решает свой спектр задач кибербезопасности:

- идентификация активов и рисков;
- защита от угроз;
- обнаружение и реагирование на угрозы;
- восстановление после реализации угрозы.

Каждый из пяти блоков может быть детализирован. Например, первый блок может включать в себя такие защитные меры, как управление защищаемыми активами и оценка рисков. Защитный блок включает в себя следующий набор мероприятий:

- контроль доступа;
- обучение и повышение осведомленности;
- защита данных;
- процедуры и процессы защиты информации и информационных систем;
- поддержка защитных мер.

Оставшиеся блоки включают в себя непрерывный мониторинг безопасности, обнаружение атак и аномалий, планирование процесса реагирования на инциденты, сбор доказательств, атрибуция кибератак, коммуникации с заинтересованными сторонами, анализ инцидента и разбор полетов, улучшение системы защиты, восстановление после сбоев и инцидентов и ряд других защитных мер.

Проанализировав известные случаи хакерских атак на гражданские ядерные объекты (ГЯО) мы пришли к выводу, что наиболее подверженной нападению является автоматическая система управления технологическим процессом (АСУ ТП).

Связь между элементами АСУ ТП осуществляется через промышленную цифровую сеть, по которой с централизованного пульта управления или с отдельных устройств для обеспечения диспетчеризации команды поступают к исполнительным устройствам или контроллерам. Обратную связь обеспечивают при помощи разнообразных датчиков. Большой информационный поток, приходящий на пункт управления ежесекундно, а также большое количество элементов системы автоматического управления и дают возможность хакерам для взлома.

Независимые исследования показывают, что практически в любой АСУ ТП можно обнаружить множественные уязвимости, которые способны привести к нарушению корректной работы технологического процесса и реализации угроз несанкционированного доступа к информации, обрабатываемой в системах диспетчерского управления и сбора данных, отдельных интерфейсах управления объектами автоматизации, элементах телеметрической подсистемы и телемеханики, прикладных приложениях для анализа производственных и технологических данных, системах управления производством.

Исходя из мирового опыта, можно обозначить следующие наиболее часто встречающиеся уязвимости:

- исполнение произвольного кода (неавторизованное, авторизованным пользователем);
- загрузка и исполнение произвольных файлов;
- отказ в обслуживании, уязвимости, вызывающие повышение привилегий;
- раскрытие информации для доступа к базе данных.

Реализация некоторых перечисленных уязвимостей позволяет остановить технологический процесс, что в реалиях АЭС и энергосистемы в целом может стать фатальным.

Ещё одной уязвимой точкой любой электростанции является её релейная защита (РЗ), цифровые устройства которой чаще всего объединены в единую сеть. При постороннем вмешательстве в работу РЗ может произойти не только перебой в снабжении потребителей электроэнергией, но и порча дорогостоящего электрооборудования АЭС, вплоть до его полного выхода из строя.

Как упоминалось выше, информационные сети электроэнергетических предприятий сталкиваются с огромным количеством потенциальных киберугроз. Такие угрозы охватывают несколько векторов атак, а каждая уязвимость имеет свою собственную стратегию защиты.

Таким образом, сеть АСУ ТП может быть реально защищена только при условии применения множества средств защиты на различных уровнях. Если коротко, только таким способом можно защитить систему от каждого вектора атак и покрыть все уязвимости, которые появляются в случае использования отдельной защитной стратегии.

Применение защитных средств на различных уровнях называется глубокой защитой. Стратегия глубокой защиты направлена не на построение непроницаемой единой стены, но на построение различных уровней защиты. Такие защитные средства используют сочетание различных тактик для того, чтобы обнаружить и заблокировать атаку.

В информационных сетях предприятий электроэнергетики такой подход должен применяться на всех уровнях и векторах потенциальных атак.

Так как АЭС является наиболее важным объектом энергетики страны, то применение стандартных межсетевых экранов и описанного выше антивирусного ПО является недостаточным для того, обеспечить глубокую защиту. Такой подход нацелен только на один вектор защиты, он окажется бесполезным, если атакующий проникнет в сеть или воспользуется вредоносным ПО для отправки вредоносных команд. По этой причине применяется стратегия многоуровневой защиты по всем векторам атак, особенно в критически важной служебной сети или сети автоматизации.

В сети АСУ ТП крупных предприятий каждый уровень глубокой защиты имеет свои преимущества и недостатки. Работая на каждом уровне, комбинированное решение успешно обеспечивает защиту от:

- удаленных атак, которые проводятся из другого местоположения. Защита достигается путем использования межсетевого экрана и межсайтового шифрования. Эти действия не позволяют хакерам получить доступ к внутренним сетям «логически»;

- атаки «человек посередине». Защита достигается путем применения межсайтового шифрования, что предотвращает повреждение или фальсификацию данных;

- атаки на уровне управления сети. Защита достигается с помощью определенной архитектуры сети. Например, выбор инфраструктуры с высокой степенью защиты, такой как *Carrier Ethernet* или *SONET/SDH* вместо *MPLS* или *MPLS-TP*;

- атаки с маскировкой. Устраняются с помощью протоколов аутентификации источника, таких как *IEEE802.1X*, которые проверяют, что определенный хост не был заменен другой машиной, которая отправляет вредоносные данные;

- перехват данных и шпионаж. Защита достигается путем использования сетевых технологий с жестким определением пути и универсальным адресным пространством – таких как *Carrier Ethernet*;

- вредоносные атаки с *RTU*, управляющих станций или *HMI*. Устраняются путем использования распределенных межсетевых экранов с распознаванием приложений. Такие межсетевые экраны могут углубленно проверять трафик *SCADA* чтобы убедиться, что команды относятся к приложению управления или автоматизации – помимо проверки, что устройства являются элементами сети автоматизации.

Должным образом разработанная сеть предприятия будет окружена множеством защитных слоев, где каждый слой нацелен на защиту от определенного типа атаки. Когда один уровень защищает от одного типа атаки, следующий уровень покрывает его уязвимости. Сеть АСУ ТП может быть полностью защищена только в том случае, когда все уровни

работают одновременно. В противном случае, каждый отдельный уровень может быть атакован и выведен из строя относительно просто.

Принципиальная схема многоуровневой защиты сети АЭС, предлагаемая для реализации, представлена на рисунке 1.



Рисунок 1 – Многоуровневая система защиты АЭС

### Литература

1. Шишов, О. В. Технические средства автоматизации и управления : учеб. пособие / О. В. Шишов. – М. : Инфра-М, 2011. – 397 с.

2. Шишов, О. В. Современные технологии промышленной автоматизации : учеб. пособие / О. В. Шишов. – Саранск : Изд-во Мордов. ун-та, 2009. – 276 с.