# ОСНОВНЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АСУ ТП КВО

*Белорусский государственный университет информатики и радиоэлектроники*
*г. Минск, Республика Беларусь*

*Бацека А. В.*

*Пачинин В. И. – канд. техн. наук, доцент*

Анализируются основные угрозы информационной безопасности современных автоматизированных систем управления (АСУ) технологическими процессами (ТП) критически важных объектов (АСУ ТП КВО). Рассматриваются мероприятия по парированию этих угроз.

Сложно переоценить безопасность автоматизированных систем управления (АСУ) технологическими процессами (ТП) критически важных объектов (АСУ ТП КВО). При этом под КВО будем понимать объекты управления, нарушение или прекращение функционирования которых наносят крупный экономический ущерб работе предприятия. Нарушения в их работе могут повлечь за собой не только нарушение или полный отказ ТП и экономические убытки, но и другие катастрофические последствия, связанные с безопасностью людей и серьезным ущербом для окружающей среды. В этой связи важно понимать, что обеспечение безопасности АСУ ТП КВО (как физической, так и информационной) — приоритетная задача для любого производства [1]. И если физическая безопасность здесь может быть решена на самом высоком уровне, то некоторые проблемы информационной безопасности (ИБ) вызывают ряд вопросов. Эти проблемы не являются уникальными для АСУ ТП КВО — они встречаются и в корпоративных сетях. Но несмотря на разную степень критичности, их распространенность в первом и втором случае несопоставима: в корпоративных сетях такие проблемы бывают решены чаще, в АСУ ТП КВО — гораздо реже. Это обусловлено несколькими заблуждениями:

- будто бы достаточно обеспечить защиту периметра АСУ ТП на логическом и физическом уровнях (межсетевое экранирование, пропускной и внутриобъектовый режим);
- якобы АСУ ТП безопасна, потому что взломщик никогда не поймет, как она работает;
- считается, что “наши АСУ ТП” не интересны для атак.

Однако угрозы информационной безопасности (ИБ) приходится парировать и для АСУ ТП КВО. Во-первых, это отсутствие своевременных обновлений программного обеспечения (ПО) из-за специфики АСУ ТП, что позволяет злоумышленникам нанести вред системе, используя известные уязвимости ПО (специфика АСУ ТП требует непрерывности ТП, поэтому для установки обновления ПО может потребоваться перезагрузка/выключение АСУ ТП).

Во-вторых, значительную угрозу представляет несовершенная парольная политика, способствующая несанкционированному доступу. Для работы на операторских/диспетчерских рабочих станциях часто используются административные учетные записи с легкими для перебора или угадывания паролями. При этом они могут быть “зашиты” весьма небезопасным способом и храниться (передаваться) в открытом виде. А иногда этих паролей может и вовсе не быть. В качестве оправдания владельцы АСУ ТП КВО обычно указывают на требование непрерывности ТП или мониторинга. По их мнению, процедуры идентификации и аутентификации пользователей (операторов и диспетчеров), которым сложно запоминать длинные пароли, могут этой непрерывности помешать.

В-третьих, мониторинг инцидентов ИБ и сетевой инфраструктуры АСУ ТП КВО часто далёк от совершенства: процессы управления инцидентами ИБ, как правило, не документированы, что мешает предприятию определить, какие события и на каких компонентах АСУ ТП должны отслеживаться, а также кто и как часто должен осуществлять их мониторинг и анализ, а отсутствие средств обнаружения вторжений не позволяет определять атаки на сетевые ресурсы и своевременно противодействовать им. Это особенно критично, если технологическая сеть подключена к корпоративной, а корпоративная — к Интернету.

В-четвёртых, существенной проблемой для безопасности АСУ ТП КВО является неосведомленность в области ИБ персонала, обслуживающего АСУ ТП. Знание и соблюдение простейших правил информационной безопасности может предотвратить как минимум реализацию непреднамеренных угроз безопасности АСУ ТП. Если даже среднестатистический «айтишник» воспринимает необходимость заниматься информационной безопасностью как досадную помеху своей работе и своего рода «геморрой» [2], то что говорить о персонале, обслуживающем АСУ ТП.

В докладе рассматриваются основные мероприятия по парированию перечисленных угроз информационной безопасности современных АСУ ТП КВО.

Список использованных источников:

1. Бацека А.В., Пачинин В.И. Анализ угроз и уязвимостей АСУ технологическими процессами // Современные средства связи: материалы XVIII Междунар. науч.-техн. конф., 15–16 окт. 2013 года, Минск, Респ. Беларусь / редкол.: А. О. Зеневич [и др.]. – Минск: УО ВГКС, 2013. – 322 с. – С. 211-213.

2. Джейкобсон Даг, Рурш Джулия. Информационная безопасность: научите персонал уважать её // Безопасность ИТ-инфраструктуры. – 2013. – № 10 (76). – С. 1-2.

Библиотека БГУИР