Александр НОВОЖИЛОВ:
«Свести к минимуму человеческий фактор»

Александр НОВОЖИЛОВ,
генеральный директор «АйТи Бастион»

С генеральным директором компании «АйТи Бастион» Connect обсудил особенности российского рынка средств контроля привилегированных пользователей.

– Какие задачи могут решать в информационной системе АСУ ТП продукты для контроля привилегированных пользователей?

– Основная задача контроля проста – свести к минимуму воздействие человеческого фактора. Наши французские коллеги рассказали, что Stuxnet – это не вирус. Был человек, который представился сервисным инженером одного из производителей АСУ ТП, и удаленно произвел действия, которые привели к катастрофе на заводе обогащения урана. Посредством наших продуктов можно быстро решать задачи обеспечения надежности, разбора инцидентов и проведения расследования.

Кроме того, контроль действий привилегированных пользователей позволяет нам выявлять нерадивых сотрудников, как собственных, так и субподрядчиков. С помощью наших продуктов можно повысить трудовую дисциплину, чтобы исполнители выполняли действия строго по инструкции, а не занимались исследованиями и самообразованием на промышленном оборудовании. Посредством контроля также можно выявить сотрудников, которые недостаточно квалифицированы. Можно осуществлять оценку качества обслуживания внешних подрядчиков и соответственно действий техподдержки производителей. Можно даже запретить наиболее очевидно опасные команды и разрешить выполнять их только высококвалифицированным пользователям. Для рядовых операторов можно обеспечить доступ к конкретному приложению, которое ему необходимо для работы, а все остальные – заблокировать.

– Какие особенности существуют у российского рынка средств контроля привилегированных пользователей?

– Российский рынок только зарождается. Это связано с тем, что рынок АСУ ТП очень консервативный. В России до сих пор существует иллюзия, что АСУ ТП отделена от других информационных систем, но практика показывает обратное. К тому же даже если человек пришел для технического обслуживания на выделенное рабочее место, то и в этом случае его необходимо контролировать.

В Европе сами производители АСУ ТП уже рекомендуют клиентам устанавливать системы контроля, чтобы избежать имиджевых рисков и конфликтных ситуаций. Российские производители АСУ ТП и даже представительства западных производителей почему-то считают, что использование такой системы позволит сотрудникам клиента ознакомиться с процессом доработки, после чего они откажутся от услуг технической поддержки. В результате заказчику не всегда хватает политической воли, чтобы убедить поставщика выполнять работы под наблюдением системы контроля.

– Насколько российским компаниям интересны продукты для контроля привилегированных пользователей?

– В России есть приказ № 31 ФСТЭК, который содержит в том числе требования по строгому контролю доступа, персонификации пользователей, контролю и фиксации их действий, причем для определенного класса АСУ ТП необходимо использовать сертифицированные решения. В некоторых случаях положения этого документа используются как корпоративные стандарты.

Наши продукты позволяют провести качественное расследование и выявить действительно виновного, а не наказывать руководителя за то, что он не обеспечил достаточного контроля. Юристы уверяют нас, что сертификата ФСТЭК на отсутствие недекларированных возможностей достаточно, чтобы записи нашего устройства можно было приобщить к показаниям в суде. У нас такой сертификат есть.

Если не говорить о катастрофах, то стоит напомнить, что на многих промышленных системах минуты простоя влекут за собой миллионные убытки, не сопоставимые со стоимостью нашей системы. Мы же позволяем ускорить разбор инцидента и сократить время решения возникшей проблемы, если она произошла по вине действий персонала в информационной системе. Причем персонал может быть из сторонней организации, выполняющей обслуживание по контракту, как это было в случае со Stuxnet. ■