# Проблемы и пути решения обеспечения информационной безопасности. Мнение разработчиков технологических систем

Важность и актуальность темы кибербезопасности в энергетике широко представлена в ежедневных новостях в СМИ. Практически «из каждого утюга» можно услышать про реализованные угрозы, кибершпионаж, исследования, проведенные экспертами в области информационной безопасности (далее – ИБ) и другое. Во многих статьях, докладах и диссертациях можно найти ряд знаменитых примеров кибератак, некоторые уже ставшие нарицательными.

**Автор**
Крутских И.В.

Приведем примеры наиболее значительных кибератак, где были выведены из строя крупные объекты, принадлежащие к критическим инфраструктурам:

- **Иран.** Сентябрь 2010 года. Реализован проект при помощи специально разработанного вируса Stuxnet, который вывел из строя почти 1000 центрифуг, предназначенных для обогащения урана. Иранским специалистам пришлось избавиться от тысячи зараженных устройств для предотвращения еще большего ущерба.[1]
- **Венесуэла.** Март 2019 года. Перебои в электроснабжении происходили 5 раз. По информации портала Netblocks.org 94 % телекоммуникационной инфраструктуры Венесуэлы вышло из строя. 90 % страны осталась без интернета. Отключение электроэнергии также произошло 6 июля 2019 г.[2] Стало известно, что система управления электростанции контролируется хакерами. В целях безопасности она была отключена.
- **Боливия 2019 год.** «Лаборатория Касперского» сделала отчет, посвященный угрозам для автоматизированной системы управления технологическими процессами (АСУ ТП). Боливия заняла второе место в мире после Ирана по количеству компьютеров, атакованных программами-вымогателями. [3]

К сожалению, в списках есть и упоминания о реализованных угрозах на территории нашей страны:

- **Россия 2014 год.** Австрийская компания «LMF» отключила две свои компрессорные станции, которые проходили испытания на объекте ПАО «Газпром». Команда отключения подавалась со спутника. Отключение можно объяснить введенными в 2014 году санкциями. В настоящее время Россия инициировала разработку аналогов, которые заменят иностранную технику. Тревогу вызывает наличие у Газпрома старых компрессоров, произведенных в США и Швейцарии. Риск их отключения остается актуальным.[4]
- **Россия 2017 год.** 21 июля 2017 г. компания «Siemens» объявила о прекращении поставок оборудования для электростанций России. Причина – «незаконное перемещение четырех газовых турбин в Крым». Важным моментом является возможность наличия в АСУ ТП импортной продукции встроенного программного обеспечения (далее ПО) будь то операционная система или прикладное ПО, которое может вызвать нарушение работы предприятий, электростанций и других, важнейших для страны объектов.[5]
- **Россия 2017 год.** «Транснефть» заявила об отказе использования оборудования «Schneider Electric», не дожидаясь своевременной реакции французов на требования устранить многочисленные уязвимости АСУ ТП, выявленные при глубоком анализе ее защищенности. Кроме этого, в 2019 году стали известны детали предполагаемых атак, в которых будет использовано кибероружие Triton, «заточенное» под оборудование «Schneider Electric».[6]
- **Россия 2018 год.** 2018 г на официальном сайте «Лаборатории Касперского» объявили о массивной атаке на свитчи Cisco, что специалисты лаборатории Касперского[7] уверены в том, что вирусные атаки на

[1] https://www.newsru.com/world/17apr2011/eas.html
[2] https://www.google.ru/search?newwindow=1&biw=1280&bih=934&ei=mqEFXqzCG8msmwWf4ZOoCg&q
[3] https://news.rambler.ru/other/42915693-opublikovan-otchet-ob-ugrozah-dlya-asu-tp-v-pervoy-polovine-2019-goda/
[4] https://www.rbc.ru/business/26/02/2020/5e5687009a79473499a36bfc
[5] https://press.siemens.com/global/en
[6] https://cnews.ru/news/top/2017-12-14_transneft_otkazalas_sotrudnichat_so_schneider
[7] https://www.kaspersky.ru/blog/cisco-apocalypse/20136/

коммутаторы Cisco направлены на российский сегмент интернета. [8]

Эти факты послужили дополнительным триггером для ответных действий регуляторов в области ИБ. Разработаны, продолжают разрабатываться и вводятся в действие законы, указы, приказы, требования и т.п. В том числе ставший одним из основных нормативных правовых актов в области обеспечения безопасности – 187-ФЗ «О безопасности критической информационной инфраструктуры». Он расширил перечень объектов (информационные системы, информационно-технологическое сопровождение (ИТС), автоматизированная система управления (АСУ), к безопасности которых выдвигается ряд обязательных требований со стороны государства, а нанесение ущерба может привести к возникновению угрозы для здоровья и жизни людей, негативно повлиять на экономическую, политическую, экологическую и социальную устойчивость региона и государства в целом. Теперь владельцы таких систем, относящихся к объектам критической информационной инфраструктуры (далее – ОКИИ), несут ответственность за их безопасность, в том числе уголовную.

Как известно, новые требования – стимул к разработке новых технологий, решений и т.д. И тут поле для деятельности открывается для всех – от методологически необходимых теоретических рассуждений до практических разработок и внедрений.

Что делать, куда бежать и за что хвататься в такой ситуации производителям технологических систем?

В первую очередь им необходимо получить себе в штат сотрудников с профильным образованием, если конечно они почему-то не сделали этого 5–10 лет назад. И это – проблема, так как несмотря на большое количество ВУЗов, выпускающих специалистов ИБ, на рынке тотальный их дефицит.

Следующий этап – внимательное изучение нормативных документов, сопоставление с документами, регламентирующими технологическую область, и в итоге – разработка или, если очень повезло, доработка решений, удовлетворяющих как специфическим отраслевым требованиям, так и требованиям в области ИБ.

Очередная проблема – вопрос выбора подхода при решении задач разработки решения, удовлетворяющего всем типам требований. По сути, выбор средств ИБ ограничен наложенными средствами, встроенными и их различные комбинации. Очевидно, что каждый вариант имеет ряд преимуществ и недостатков. Наложенные средства, по сути, новый специфический элемент системы, а значит, они должны удовлетворять некоторым требованиям, в том числе:

- совместимость с технологической системой;
- отсутствие снижения быстродействия;
- отсутствие негативного влияния на выполнение целевой функции технологической системы;
- работоспособность в промышленных условиях.

Встроенные же средства, по определению, внедряются, дорабатываются, испытываются и вводятся в эксплуатацию в составе технологической системы, являясь ее неотъемлемой частью, а значит полностью удовлетворяют вышеуказанным требованиям. Встроенные средства – неотъемлемая часть, в отличии от наложенных средств. Но разработка таких решений, в свою очередь, требует от производителя опять же квалифицированных кадров, опыта разработки, наличие соответствующих лицензий и др. Дополнительным положительным фактом может являться стоимость встроенных решений, в сравнении с наложенными средствами.

За безотказную работу системы отвечать ее разработчику, и все чаще можно услышать просьбу последнего: «Не надо защищать нас без нас». Поэтому многие вендоры строят свои системы в большинстве своем с встроенными механизмами защиты, понимая, что именно такой подход экономически и функционально выгодный.

Тем не менее часть системы ИБ в настоящее время чаще всего все же остаются наложенными, в том числе – анализ защищенности, антивирусная защита, SIEM. Это обусловлено прежде всего большими объемами необходимых инвестиций, специализированной экспертизы и затрат на разработку таких подсистем.

В то же время применение наложенных подсистем на практике сопровождается несколькими итерациями совместных испытаний и совместных доработок. И здесь стоит сказать, что многие вендоры систем ИБ еще не оценили финансовый и технологический потенциал совместных решений с вендорами технологических систем, и потому стороны пока слабо идут на контакт.

Если вдаваться в частности, то в качестве встроенных средств защиты информации чаще всего используются:

- система идентификации и аутентификации;
- система регистрации событий ИБ;
- криптографические средства;
- средства обнаружения вторжений;
- межсетевые экраны;
- и отдельно выделенный класс – операционные системы.

При разработке большинство производителей старается сразу правильно выстроить технологический процесс разработки, неизбежно приходится внедрять системы и новые технологии,[9] такие как:

- внедрение безопасной разработки, соответствие стандарту МЭК 62443-4-1;
- переход к облачным технологиям.

В качестве основных преимуществ подхода с использованием встроенных/комбинированных средств выделим следующие:

- документирование всех функций защиты информации, реализованных в продуктах;
- реализация функций защиты информации, встроенных непосредственно в устройства различных уровней технологических систем – экономически и функционально выгодно;
- заказчик получает одного исполнителя, отвечающего за всю защищенную технологическую систему;

В заключении стоит отметить, что при разработке систем, в которых тесно взаимодействуют технологические системы и системы обеспечения ИБ, комплексный подход позволит значительно упростить проектирование, внедрение и дальнейшую эксплуатацию спроектированных объектов. А сама подсистема ИБ, скорее всего, должна стать одной из технологических подсистем.

При таком подходе решается одна из основных проблем – корректность взаимодействия компонентов технологических систем и наложенных средств защиты информации. Также необходимо принять во внимание, что такие системы находятся на гарантийном или сервисном обслуживании и внедрение дополнительных средств защиты информации требует получения одобрения производителя оборудования, которое под каждый новый проект влечет крупные временные затраты на согласование решений, проведение испытаний, устранение замечаний.

[8] https://ria.ru/20180407/1518127365.html?referrer_block=index_archive_16

[9] Журнал «Релейщик», № 1, 2020, стр. 60–62.

**Крутских И.В.,** генеральный директор ООО «ПиЭлСи Технолоджи»