PCWEEK RUSSIAN EDITION REVIEW
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И РЕШЕНИЯ ДЛЯ БИЗНЕСА
ИТ-БЕЗОПАСНОСТЬ
СЕНТЯБРЬ • 2013 • МОСКВА
http://www.pcweek.ru

Информационная безопасность критически важных объектов

ВАЛЕРИЙ ВАСИЛЬЕВ

Недавние кибератаки Stuxnet, Duqu, Flame, Gauss и другие им аналогичные показали, насколько уязвимы ИТ-инфраструктуры топливно-энергетических, производственных, транспортных, инфотелекоммуникационных, коммунальных, финансовых и других систем жизнеобеспечения людей и насколько катастрофичными могут быть последствия вызванных подобными атаками сбоев и отказов в их работе.

ОБЗОРЫ

Согласно данным аналитической компании Secunia, информационная безопасность (ИБ) программной составляющей АСУ ТП, которые представляют собой специфический компонент, присущий ИТ-инфраструктурам многих критически важных объектов (КВО), более чем на десять лет отстает от состояния ИБ наиболее распространенного современного ПО.

В нашем обзоре мы постарались осветить реальное состояние дел в указанной области и перспективы решения сложностей с обеспечением ИБ информационных систем, поддерживающих технологические процессы КВО.

Критерии защищенности ИТ-инфраструктур КВО

В соответствии с распоряжением Правительства РФ от 23.03.2006 № 411-рс, как напоминает Андрей Степаненко, к критически важным относятся совершенно разные по своему предназначению объекты — магистральные сети связи, системы телерадиовещания, заводы, электростанции, предприятия нефте- и газодобычи, транспортная инфраструктура и т. п. Столь различные объекты имеют слишком разные ИТ-системы, поэтому универсальных критериев защищенности ИТ-инфраструктур КВО, как полагает г-н Степаненко, скорее всего, не существует — они должны определяться для КВО, сходных по назначению и архитектуре.

Тем не менее наши эксперты находят и общие черты в обеспечении ИБ ИТ-инфраструктуры КВО. Алексей Косихин подходит к оценке уровня защищенности ИТ-инфраструктур КВО с позиции надежности и защищенности тех узлов, получив доступ к которым, злоумышленник может нанести наибольший вред. Поэтому наивысший приоритет в защите ИТ-инфраструктур КВО, как он считает, имеют: защита периметра; разграничение доступа к критичным серверам; защита серверов управления и рабочих станций, которые управляют АСУ ТП; защита критичных контроллеров АСУ ТП. Обеспечение их ИБ позволяет нивелировать последствия большинства угроз.

Владимир Бычек рассматривает типовую топологию КВО как совокупность подсистем, сегментированных (в большинстве случаев) посредством межсетевых экранов. Это корпоративная сеть передачи данных и технологическая сеть (где проходят технологические процессы; из нее в ряде случаев выделяют как самостоятельную диспетчерскую сеть, служащую для управления технологическими процессами).

Критерии защищенности ИТ-инфраструктуры КВО г-н Бычек формулирует так:

- постоянный контроль соединений между подсистемами, исключение соединений и блокирование сервисов, которые не являются необходимыми для функционирования КВО в штатном режиме;
- обеспечение максимального уровня ИБ соединений, необходимых для функционирования КВО;
- регулярный технический аудит элементов, сетей КВО и подключенных сетей для выявления проблем ИБ;
- документирование инфраструктуры КВО, выделение элементов и подсистем, требующих дополнительных уровней защиты;
- строгий и непрерывный процесс управления рисками;
- наличие регламентов, описывающих процессы внесения изменений в инфраструктуру КВО и контроль их выполнения.

По мнению Руслана Стефанова, для оценки защищенности КВО можно применять три критерия: соответствие уровня ИБ КВО некому целевому уровню ИБ; выполнение принципа "чёрного ящика", когда исключается любое внешнее воздействие на информационную систему и при этом информация об объекте не покидает её пределов информационной системы; количество инцидентов.

Характеризуя целевые уровни ИБ, г-н Стефанов ссылается на стандарт IEC 62443—1-1, предлагающий следующие варианты уровней:

- уровень ИБ 0 — требования к информационной безопасности отсутствуют;
- уровень ИБ 1 — для защиты от случайных или непреднамеренных нарушений (угроз);
- уровень ИБ 2 — для защиты от преднамеренных нарушений (угроз) с применением простых средств и минимальных ресурсов, требующих общих навыков и минимальной мотивации;
- уровень ИБ 3 — защита от преднамеренных нарушений (угроз) с применением сложных средств и умеренных ресурсов, требующих специфичных для объекта защиты навыков и умеренной мотивации;
- уровень ИБ 4 — защита от преднамеренных нарушений (угроз) с применением сложных средств и максимальных ресурсов, требующих специфичных для объекта защиты навыков и максимальной мотивации.

В качестве наиболее важных Аркадий Прокудин выделяет следующие меры обеспечения ИБ КВО (их принятие одновременно служит критериями ИБ КВО): наличие политики ИБ для персонала КВО и тех, кто сотрудничает с ним; идентификация и аутентификация пользователей в информационных системах КВО; регистрация и учет событий в ИТ- и ИБ-системах для мониторинга и расследования инцидентов; контроль корректности функционирования ИТ-сервисов; непрерывность защиты сервисов КВО.

ИБ-риски, специфичные для КВО

Главной особенностью КВО является использование специализированных АСУ ТП. В проекте закона "О безопасности критической информационной инфраструктуры Российской Федерации" АСУ ТП определяется как комплекс аппаратных и программных средств, информационных систем и информационно-телекоммуникационных сетей, предназначенных для решения задач оперативного управления и контроля за различными процессами и техническими объектами в рамках организации производства или технологического процесса КВО. Именно на обеспечении ИБ АСУ ТП КВО и предлагают наши эксперты сосредотачивать главные усилия при организации ИБ ИТ-инфраструктуры КВО.

Как отмечает г-н Степаненко, ранжирование рисков по возможным последствиям — непростая задача, тем более в применении к столь разным по своему назначению КВО. В большинстве документов (например, в отчете Risk assessment methodologies for critical infrastructure protection. Part I: A state of the art, подготовленном по заданию Еврокомиссии в 2012 г., содержится краткий обзор 21 документа по управлению рисками КВО в разных странах) риски для КВО группируются по трём категориям: физические (связанные с природными катастрофами и т. п.), человеческие (ошибки персонала и пр.) и киберриски. Именно киберриски в последние годы рассматриваются как наиболее критичные для КВО, которые становятся объектами атак кибертеррористов и иностранных спецслужб.

Специфику ИТ-инфраструктуры КВО (и прежде всего АСУ ТП КВО) Андрей Духвалов видит в том, что она одновременно подвергается как обычным угрозам (например, заражению вирусами), так и целевым кибератакам (APT) и потому должна иметь защиту от распространенных вредоносов и при этом располагать специальными ИБ-средствами и ИБ-политиками для противодействия таргетированным атакам.

Наиболее опасные риски г-н Косихин связывает с проникновением внешнего нарушителя внутрь ИТ-периметра КВО, особенно когда дело касается APT-атак на системы управления АСУ ТП.

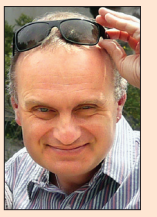
К числу специфичных г-н Косихин относит риски, связанные с использованием неадаптированных ИБ-средств, что тоже может нарушить работу КВО. Например, большинство антивирусов опознают данные протоколов, по которым работают АСУ ТП, как вредоносный код и блокируют их.

Алексей Косихин отмечает, что существуют риски, связанные с архитектурными особенностями АСУ ТП. Например, риск взлома извне более вероятен для системы, реализованной на современной промышленной платформе, что он связывает с расширенным списком лиц, имеющих к ней доступ: наряду с персоналом владельца АСУ ТП это могут быть представители вендора (удаленно обновляющие и поддерживающие платформу) и специалисты интегратора (внедряющие платформу). Если же АСУ ТП работает на платформе, разработанной индивидуально, есть риск снижения её работоспособности, связанный с невозможностью оперативно устранять неполадки в силу отсутствия на рынке специалистов нужной квалификации.

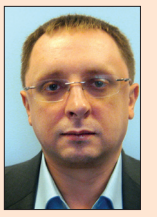
Руслан Стефанов предлагает разделять ИБ-риски для КВО на две группы: риски общие, присущие всем объектам, и специфичные для отрасли, к которой от-

ПРОДОЛЖЕНИЕ НА С. 20 ▸

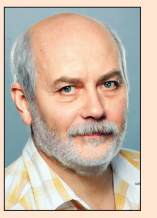
Наши эксперты



ВЛАДИМИР БЫЧЕК, *руководитель направления сетевой безопасности, IITD Group*



ВЛАДИМИР ВАКАЦИЕНКО, *технический эксперт RSA, "EMC Россия и СНГ"*



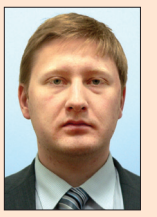
АНДРЕЙ ДУХВАЛОВ, *стратег по развитию технологий "Лаборатории Касперского"*

АЛЕКСЕЙ КОСИХИН, *руководитель направления по работе с ТЭК Центра информационной безопасности, "Инфосистемы Джет"*

АРКАДИЙ ПРОКУДИН, *заместитель руководителя отдела информационной безопасности, "АйТи"*

АНДРЕЙ СТЕПАНЕНКО, *директор по маркетингу, "Код Безопасности"*

РУСЛАН СТЕФАНОВ, *руководитель направления защиты АСУ ТП, "Элвис Плюс"*



ВЛАДИМИР ЧЕРКАСОВ, *старший консультант, "Информзащита"*

Информационная безопасность АСУ ТП КВО. Основные проблемы

ВЛАДИМИР ЧЕРКАСОВ

Сложно переоценить безопасность автоматизированных систем управления технологическими процессами критически важных объектов (АСУ ТП КВО). Нарушения в их работе могут повлечь за собой не только нарушение или полный отказ технологического процесса 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. 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 чаще бывают решены, 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.

По статистике NIST (National Institute of Standards and Technology), опубликованной в "Руководстве по безопасности автоматизированных систем управления" (Guide to Industrial Control Systems (ICS) Security, Special publication 800—82), самыми опасными являются нацеленные внешние атаки. Хотя при этом они и самые малочисленные. Наиболее вероятными считаются непреднамеренные угрозы и рассерженные сотрудники, в том числе и бывшие.

Обновление программного обеспечения

Как правило, установка обновлений безопасности на компоненты АСУ ТП осуществляется очень редко. Обусловлено это несколькими факторами:

- необходимость непрерывности технологического процесса (для установки обновления может потребоваться перезагрузка/выключение АСУ ТП);
- недопустимость автоматического обновления и необходимость предварительного тестирования обновлений в силу критичности АСУ ТП КВО;
- зависимость от разработчика программного обеспечения АСУ ТП.

Отсутствие своевременных обновлений позволяет злоумышленникам нанести вред системе, используя известные уязвимости ПО. Для всех системных компонентов и ПО должны быть установлены самые последние обновления безопасности, предоставленные производителями.

Управление доступом и парольная политика

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.

Таким образом, достаточно получить физический доступ к данному компоненту АСУ ТП, чтобы в дальнейшем скомпрометировать всю систему. В качестве оправдания владельцы АСУ ТП КВО обычно указывают на требование непрерывности технологического (производственного) процесса или мониторинга. По их мнению, процедуры идентификации и аутентификации пользователей (операторов и диспетчеров), которым сложно запоминать длинные пароли, могут этой непрерывности помешать. В качестве компенсационной меры они считают достаточной организацию строгого пропускного и внутриобъектового режима.

Но действительно ли этого достаточно? Чтобы ответить на данный вопрос, можно вспомнить внутренних нарушителей, социальную инженерию, а также обычные вирусные заражения, которые могут привести к плачевным результатам.

Управление инцидентами

Процессы управления инцидентами ИБ, как правило, не документированы и не осуществляются должным образом. Между тем предприятию необходимо определить, какие события и на каких компонентах АСУ ТП должны отслеживаться, а также кто и как часто должен осуществлять их мониторинг и анализ.

Характерный пример: по результатам оценки рисков установка ограничений по количеству попыток ввода пароля может быть признана опасной с точки зрения обеспечения непрерывности технологического процесса. Но в таком случае в качестве компенсационной меры обязательно должен вестись мониторинг событий неправильного ввода пароля. Эта мера может помочь своевременно выявить заражение компонентов АСУ ТП вредоносным ПО, которое часто сопровождается попытками подбора паролей для дальнейшего заражения и распространения.

Отсутствие системы мониторинга ИБ-событий и реагирования на инциденты не позволяет оперативно отслеживать возникающие критические события и деструктивные действия злоумышленников, чтобы своевременно принять необходимые и адекватные меры противодействия. Вместе с тем организацию системы централизованного сбора и анализа событий ИБ сложно отнести к дорогостоящим процедурам. По крайней мере она не требует покупки программно-аппаратных комплексов, которые стоят больших денег.

Мониторинг сетевой инфраструктуры АСУ ТП

Мониторинг сетевой инфраструктуры АСУ ТП КВО часто ограничивается выявлением неисправностей или сбоев сетевого оборудования. В отсутствие средств обнаружения вторжений невозможно определять атаки на сетевые ресурсы и своевременно противодействовать им. Это особенно критично, если технологическая сеть подключена к корпоративной, а корпоративная — к Интернету.

С учетом требований к непрерывности технологических процессов рекомендуется использовать системы пассивного обнаружения вторжений, которые будут осуществлять анализ сетевого трафика без вмешательства в процессы передачи данных.

Осведомленность сотрудников в области ИБ

Еще одной 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. А осознание того, что служба безопасности отслеживает и контролирует действия обслуживающего персонала, может снизить вероятность реализации преднамеренных угроз.

* * *

Отмеченные выше ИБ-проблемы не исчерпывают весь перечень. Вместе с тем нужно отметить, что владельцы АСУ ТП КВО, отечественные и зарубежные регуляторы, ИБ-интеграторы все чаще правильно оценивают их критичность и необходимость решать их.

Автор статьи — старший консультант компании "Информзащита".

Информационная...

◂ ПРОДОЛЖЕНИЕ СО С. 19

носится КВО. Кроме этих групп он разделяет риски, характерные для самого объекта защиты, и риски для его окружения. Например, при аварии на КВО могут пострадать не только люди, непосредственно работающие на нём, но и те, кто живёт рядом с объектом.

К наиболее критичным для АСУ ТП КВО Владимир Черкасов относит риски, связанные с нарушением целостности (модификацией) и доступности управляющей информации, что отличает АСУ ТП от корпоративных информационных систем, для которых на первом месте обычно стоит обеспечение конфиденциальности данных.

Наиболее уязвимые компоненты ИТ-инфраструктуры КВО

Наиболее уязвимым г-н Косихин признает внешний периметр ИТ-инфраструктуры КВО, так как на него приходится, как он считает, львиная доля атак, направленных на взлом АСУ ТП. И во вторую очередь уязвимы серверы управления как критичный элемент ИТ-инфраструктуры, отвечающий за работу всей АСУ.

Руслан Стефанов, в свою очередь, обращает внимание на защиту АРМ операторов технологических процессов. Ссылаясь на статистику, он утверждает, что именно эти рабочие места являются самыми уязвимыми, что связано прежде всего с режимом их функционирования. Они должны работать круглосуточно, не оставляя времени на обновление операционных систем, прикладного и защитного ПО. Поэтому такие обновления осуществляются только во время технологических окон, которые могут появляться всего один-два раза в год. К распространённой уязвимости АРМ г-н Стефанов относит также низкую сложность или полное отсутствие паролей доступа. Аудиты и тесты на проникновение, в которых он принимал участие, показывают, что подобрать пароль для АРМ несложно.

Другим возможным вектором атаки является общая для корпоративных и технологических сервисов и информационных систем сетевая инфраструктура. Такая ситуация позволяет злоумышленнику атаковать технологическую сеть из корпоративной и наоборот. Уязвимости сетевого оборудования хорошо описаны, а ограничения на обновления ПО на нём такие же, как и на АРМ операторов ТП.

Виртуализация пока нешироко применяется на КВО, но тенденции в сфере ИТ говорят о том, что в скором времени и там станут актуальными угрозы, специфичные для виртуализированных сред: в случае использования технологических и прочих ИТ-ресурсов в единой виртуальной среде возникают угрозы проникновения из корпоративных сегментов в технологические через общую платформу виртуализации.

Негативно эксперты оценивают ситуацию с удалённым доступом и управлением. Некоторые операции по обслуживанию систем отдаются на аутсорсинг, и если систему "корпоративная сеть — аутсорсер" можно считать защищенной, то гарантировать защищённость ИТ-среды аутсорсера сложно. Это создает ещё один вектор атак на ИТ-инфраструктуру КВО.

Наиболее уязвимыми компонентами ИТ-инфраструктуры КВО г-н Духвалов признает программируемые логические контроллеры и АСУ ТП в целом. Типичной уязвимостью контроллеров являются их нестойкость к сетевым атакам вроде DoS/DDoS и обычно задаваемые их производителями и оставляемые без изменений владельцами (в целях удобства последующего обслуживания и поддержки) логин и пароль администратора. Только в открытых источниках указано около 650 уязвимостей в АСУ ТП, и их число неуклонно растет.

Факторы, затрудняющие защиту ИТ-инфраструктур КВО

Согласно наблюдениям г-на Бычека, инфраструктуры КВО, как правило, представляют собой крупные распределенные сети, объединяющие сегменты различных типов. При этом не реализуется прозрачность — возможность увидеть инфраструктуру в целом, учитывая взаимное влияние всех сегментов друг на друга. Это затрудняет оценку защищенности КВО и разработку рекомендаций по ее укреплению.

Распространенной практикой сегодня стало совместное использование унаследованных систем и протоколов с современными системами, поддерживающими IP. ИТ-инфраструктура КВО чувствительна к ошибкам в конфигурировании, в том числе сетевого оборудования. В подавляющем большинстве случаев активное сканирование элементов КВО невозможно из-за риска вывода систем из строя.

Владимир Бычек отмечает также недостаточную для защиты КВО эффективность современных ИБ-систем, работающих в режиме реального времени: в АСУ ТП даже самой быстрой реакции на ИБ-инцидент может оказаться недостаточно для предотвращения вероятных последствий инцидентов. В большинстве случаев невозможно устранить известные уязвимости в настройках и ПО из-за строгих регламентов эксплуатации систем, требующих длительного согласования любых, особенно потенциально опасных действий над их элементами.

Алексею Косихину в своей практике чаще всего приходится сталкиваться с организационными трудностями в построении ИБ ИТ-инфраструктуры КВО: ИБ-специалистам не всегда предоставляется физический доступ к КВО, нередко необходимы специальные разрешения на допуск, что может быть связано с дополнительным инструктажем, обучением, экзаменами и т. п. Даже наличие контракта с заказчиком не всегда облегчает доступ экспертов на обследуемые площадки.

Из архитектурных сложностей г-н Косихин отмечает территориальную разнесенность КВО; в то же время для того чтобы понять архитектуру, необходимо оценку ситуации проводить именно на местах: как осуществляется допуск к элементам АСУ ТП с серверов и рабочих станций, как расположены контроллеры, как они друг с другом взаимодействуют...

Среди технологических проблем г-н Косихин выделяет использование ИБ-средств, не адаптированных к протоколам, по которым работает большинство АСУ ТП. В этом случае приходится продумывать общую архитектуру системы защиты таким образом, чтобы минимизировать возникающие риски иными средствами, например разграничением физического доступа сотрудников, расширенным логированием и т. п.

Со своей стороны г-н Стефанов к технологическим проблемам относит ограничения, связанные с непрерывным функционированием АСУ ТП в круглосуточном режиме. Организационные ограничения, на его взгляд, связаны с тем, что службы ИТ и эксплуатации АСУ ТП имеют отличные от службы ИБ приоритеты. У одних это доступность информационных ресурсов и непрерывность работы, у других — обеспечение ИБ. Ещё ▸

одна сложность — длительная процедура согласования любых работ между многочисленными службами, включая обслуживающие компании-аутсорсеры.

К архитектурным факторам, затрудняющим защиту ИТ-инфраструктур КВО, Владимир Черкасов относит необходимость взаимодействия сетей АСУ ТП с корпоративными сетями передачи данных, что обусловлено все более тесной интеграцией процессов управления ТП и корпоративного управления. В связи с этим приходится дополнительно решать вопросы обеспечения ИБ межсетевого взаимодействия.

То, что заказчики отдают предпочтение готовым программно-аппаратным комплексам известных разработчиков, а не разрабатывают АСУ ТП под себя с нуля, делает общедоступной информацию об архитектуре АСУ ТП, о порядке обслуживания, о возможностях подключения, уязвимостях и т. д., что также отрицательно сказывается на ИБ ИТ-инфраструктуры КВО.

По мнению г-на Черкасова, на этапах разработки и внедрения АСУ ТП часто не обращают внимания на ИБ-проблемы, что существенно затрудняет реализацию ИБ на этапе эксплуатации. Иногда разработчики и интеграторы АСУ ТП побуждают владельцев систем использовать конкретные средства защиты, запрещая вносить какие-либо изменения в свои платформы под угрозой снятия заказчиков с сервисного обслуживания. Это также затрудняет внедрение эффективной комплексной системы защиты.

Специальные средства защиты ИТ-инфраструктур КВО

Как считает г-н Бычек, для эффективной защиты ИТ-инфраструктуры КВО нужны дополнительные специальные ИБ-средства, в которых должны быть учтены критерии их защищенности и факторы, затрудняющие процесс их защиты. Это проактивные аналитические системы, позволяющие неинтрузивными методами анализировать инфраструктуру КВО и иметь средства для построения ее виртуальной модели, учитывающей конфигурацию сетеобразующих устройств (маршрутизаторов, балансировщиков нагрузки и т. д.), сегментирующих устройств и ИБ-систем (межсетевых экранов, IPS и т. д.), хостов, контроллеров и других элементов КВО. Они должны поставлять информацию об угрозах и уязвимостях, иметь средства автоматизации процесса анализа рисков, приоритизации уязвимостей, составления эффективного плана минимизации рисков до приемлемого уровня, построения рабочего процесса таким образом, чтобы выполнялись установленные регламенты по внесению изменений в инфраструктуру КВО и устройства, обеспечивающие информационный ее обмен с другими сетями (бизнес-сетями, Интернетом, сетями партнеров и т. д.).

По мнению г-на Косихина, для ИТ-инфраструктуры КВО можно эффективно использовать и системы защиты, применяемые для стандартных ИТ-инфраструктур, хотя некоторых функциональных возможностей в них не хватает, а некоторые, наоборот, избыточны применительно к АСУ ТП. Так, и в ИТ-инфраструктуре КВО необходимо разграничивать доступ к ее элементам, вести контроль целостности ПО, обеспечивать защиту от использования съемных носителей и т. п., но при этом совершенно не нужно, допустим, контролировать утечки конфиденциальной информации. В то же время применяемые ИБ-средства должны распознавать специфичные для АСУ ТП сетевые протоколы.

Большинство представленных на российском рынке ИБ-продуктов адаптированы для защиты зарубежных АСУ ТП, но не сертифицированы по требованиям нашего законодательства, поскольку зарубежные вендоры не всегда готовы предоставлять исходные программные коды своих продуктов, что необходимо для сертификации. Отечественных же ИБ-решений требуемого уровня, как считает г-н Косихин, пока нет.

Руслан Стефанов отмечает две основные тенденции в НИОКР в сфере ИБ АСУ ТП. Первая — встраивание средств обеспечения ИБ непосредственно в технологическую среду (контроллеры, исполняющие устройства, пункты технологического и диспетчерского управления, специализированное ПО) на стадии проектирования и производства. Это позволяет учесть специфику функционирования АСУ ТП и отказаться от использования наложенных ИБ-средств.

Вторая тенденция — исследования в области “умных” обновлений ПО. Такие обновления должны вести себя предсказуемо при установке, корректно наследовать настройки и устанавливаться без остановки технологического процесса. Согласно наблюдениям г-на Стефанова, уже есть проекты АСУ ТП, которые сами следят за корректностью установки обновлений ПО.

История с вирусом Stuxnet показала, что гарантированно защититься от целенаправленных кибератак невозможно. Поэтому, по мнению Владимира Вакациенко, нужно внедрять стандартные организационно-технические методы обеспечения ИБ. Необходимы также средства, которые позволят контролировать события во всей ИТ-инфраструктуре КВО, а не только в АСУ ТП, и своевременно выявлять аномалии.

Владимир Черкасов отмечает, что на рынке есть ИБ-средства, “заточенные” под особенности АСУ ТП, — специализированные межсетевые экраны, средства защиты межсетевого взаимодействия типа “диодов данных” (Data diode), обеспечивающие на физическом уровне однонаправленную передачу данных между технологическим сегментом и остальной корпоративной сетью. При этом, напоминает он, нельзя категорично утверждать, что обычные средства защиты межсетевого взаимодействия, настроенные должным образом, не могут применяться в сетях АСУ ТП в тех же целях.

Состояние защищенности ИТ-инфраструктуры КВО в России

Готова ли ИБ-индустрия обеспечить полноценную защиту инфраструктуры российских КВО? Главную проблему здесь г-н Степаненко видит в том, что потенциальный для объектов КВО злоумышленник, скорее всего, обладает высоким профессионализмом и использует целевые атаки, а наработанной практики противодействия таким атакам в нашей стране практически нет. Именно поэтому для многих КВО их АСУ ТП проектируются изолированно от внешних систем.

Владимир Бычек оптимистично смотрит на перспективы российского ИБ-рынка с точки зрения его потенциальной способности обеспечить ИБ АСУ ТП. По его наблюдениям, практически все российские ИБ-интеграторы испытывают большой интерес к защите инфраструктур КВО, наращивают компетенции в этой области, изучают рынок подходящих решений. Разработчики средств борьбы с вредоносным кодом, как и вендоры сканеров безопасности, работают над выявлением уязвимостей в специфических элементах инфраструктуры КВО, пробуют свои силы в аудите их ИБ. На рынке появились и быстрыми темпами совершенствуются новые системы обеспечения ИБ инфраструктур КВО.

ИБ-интеграторы, считает и г-н Косихин, уже сейчас могут обеспечить необходимый для КВО уровень защиты, даже применяя для этого ИБ-средства, не адаптированные под их специфику. Однако отечественных продуктов, ориентированных на защиту промышленных АСУ, по его наблюдениям, крайне мало. Хотя в последние два года многие российские разработчики озаботились выпуском ИБ-продуктов такого класса, способных конкурировать с зарубежными аналогами, большинство из них пока находятся в стадии разработки или пилотных испытаний, а на рынке появятся года через два-три.

Состояние российской регулятивной базы для области ИБ КВО

Андрей Степаненко с сожалением констатирует, что готовой нормативной базы в нашей стране для этой области нет. Наши регуляторы все еще существенно отстают от своих зарубежных коллег, например из США и стран Европы, где уже действует ряд нормативных документов, причем привязанных к конкретным отраслям, в то время как у нас только обсуждается проект закона “О безопасности критической информационной инфраструктуры Российской Федерации”.

Руслан Стефанов считает, что российскому ИБ-рынку сегодня понятно, куда двигаться в области обеспечения ИБ КВО. Он отмечает, что почти готовы документы верхнего уровня, которые определяют общие положения организации ИБ АСУ ТП. Но остается много вопросов по нормативным документам нижнего уровня, определяющим, как достигать указанных целей. В такой ситуации специалистам приходится полагаться на собственный опыт.

Алексей Косихин отмечает, что в настоящее время специалисты руководствуются рекомендациями ФСТЭК РФ от 2005 — 2007 гг., рассчитанными на ключевые системы информационной инфраструктуры, которые, по его мнению, в принципе и являются КВО. Однако обязательность исполнения этих рекомендаций законодательно не закреплена.

Непосредственно в области регулирования ИБ КВО г-н Черкасов выделяет несколько нормативных документов:

- “Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации (утвержден Президентом РФ 12.02. 2012);
- федеральный закон № 256-ФЗ от 21.06.2011 “О безопасности топливно-энергетического комплекса” (частный случай КВО);
- “Система признаков КВО и критериев отнесения функционирующих в их составе информационно-телекоммуникационных систем к числу защищаемых от деструктивных информационных воздействий” (Совет безопасности, 08.11.2005);
- проект ФЗ “О безопасности критической информационной инфраструктуры Российской Федерации”;
- методические документы ФСТЭК РФ по обеспечению безопасности информации в ключевых системах информационной инфраструктуры (2007 г.).

Первые четыре документа г-н Черкасов относит к высокоуровневым, определяющим государственную политику, основные принципы и методы государственного регулирования в данной сфере. Методические документы ФСТЭК по обеспечению безопасности информации в ключевых системах информационной инфраструктуры содержат, на его взгляд, конкретные детализированные требования и методы обеспечения ИБ КВО, а также рекомендации по их выполнению. Но и они уже требуют актуализации, поскольку существуют пять лет, а в ИТ и ИБ это большой срок.

Аркадий Прокудин оценивает состояние нормативной базы, относящейся к области ИБ КВО, как сформированной частично. Есть, например, документы Совета безопасности РФ и ФСТЭК, трактующие подходы к организации защиты КВО, но неясно, как обстоят дела с выполнением плана, опубликованного в документе “Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами…”. В нем выделены следующие этапы:

- 2012—2013 гг. — первичное планирование и определение бюджета;
- 2014—2016 гг. — выпуск основных нормативных документов, проведение первоочередных мероприятий, разработка комплексных систем защиты, ввод первой очереди ситуационного центра единой государственной системы обнаружения и предупреждения компьютерных атак, создание сил и средств ликвидации последствий инцидентов;
- 2017 г. — основные внедрения систем и их поддержка.

Таким образом, в том, что касается совершенствования нормативной базы ИБ КВО, предстоит еще большая работа, но это вполне типичная для ИТ-индустрии ситуация, обусловленная свойственными ей быстрыми темпами технологических изменений.