15 ➔ Опрошенные BG руководители российских компаний, работающих в сфере ИБ, фиксируют рост киберугроз, направленных на предприятия топливно-энергетического комплекса, отмечая, что на их долю приходится 10–15% от общего объема рынка ИБ в России.

«Абсолютно все энергетические компании сейчас уделяют пристальное внимание защите своих объектов. Это связано с объективными причинами: вывод из строя объекта энергетики можно приравнять к терроризму, потому что это способно парализовать деятельность целого района или населенного пункта. Также это относится и к разработке ряда нормативных документов, регулирующих работу в этом направлении»,— объясняет руководитель направления по информационной безопасности СЗФО департамента информационной безопасности компании Softline Алексей Богомолов. В частности, по его словам, в 2014 году был выпущен 31 приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК), в котором прописаны требования к обеспечению защиты критически важных объектов.

По данным «Лаборатории Касперского» (ЛК), энергетика в мире оказалась на пятом месте среди атакованных отраслей (после производства, инжиниринга, образования, пищевой промышленности). «Например, американский центр реагирования на инциденты в промышленности ICS-CERT опубликовал информацию о 290 зарегистрированных случаев в США, среди которых 59 инцидентов в энергетике. По нашим данным, в течение первого полугодия 2017 года во всем мире защитными решениями ЛК были предотвращены попытки атак на 37,6% компьютеров АСУ (автоматизированные системы управления). В России этот показатель составил 42,9%»,— комментирует руководитель проекта по развитию решений по безопасности критической инфраструктуры ЛК Антон Шипулин.

Кроме того, по его словам, в этом году ЛК провела глобальный опрос о состоянии кибербезопасности среди 359 специалистов промышленных предприятий в 21 стране мире. Среди прочего было заявлено, что каждая вторая промышленная компания в мире пережила от одного до пяти киберинцидентов, также участились заявления официальных лиц государств о попытках атак на промышленные объекты, включая электроэнергетику. Господин Шипулин прогнозирует, что в сфере промышленной безопасности в 2018 году интенсивность киберугроз будет не меньше, чем в 2017-м.

В компании ESET Russia подтверждают, что в течение этого года возросло число кибератак на энергетические объекты. «Среди них как массовые атаки по классическим сценариям (такие как спам с вредоносными вложениями), так и сложные таргетированные атаки»,— говорит руководитель поддержки продаж ESET Russia Виталий Земских. К их числу компания относит выявленную в июне вредоносную программу Industroyer, специально разработанную для атак на компании электроэнергетического сектора.

«Industroyer позволяет напрямую управлять выключателями и прерывателями цепи на подстанциях, а также проводить атаки типа „отказ в обслуживании“ (DoS) на устройства релейной защиты (в частности, линейку Siemens Siprotec). Программа взаимодействует с протоколами промышленной связи, широко распространенными в энергетике. Эти протоколы создавались десятилетия назад без учета требований безопасности, поэтому поиск уязвимостей для работы в них не требуется — Industroyer просто использует протоколы по прямому назначению. Авторы Industroyer могут перенастроить программу, чтобы атаковать любую промышленную среду, где используются целевые протоколы связи. Возможные последствия подобной атаки — от перебоев в электроснабжении до физического повреждения оборудования»,— поясняет господин Земских. Он предполагает, что программный комплекс, подобный Industroyer, мог стать причиной отключения электроэнергии в Киеве в декабре 2016 года. Версия вероятна, поскольку программа имеет соответствующий функционал, а также содержит метку времени активации, совпадающую с днем блэкаута.

Партнер EY, руководитель направления по предоставлению услуг в области бизнес-рисков, управления IT и кибербезопасности в СНГ Николай Самодаев отмечает, что ущерб от реализовавшихся рисков ИБ в энергосекторе вырос. «Так, если в 2016 году только 38% респондентов (международного исследования EY по вопросам информационной безопасности.— BG) отметили, что ущерб от инцидентов ИБ превысил отметку в $100 тыс., то в 2017 это количество респондентов увеличилось до 47%»,— говорит господин Самодаев.

САМЫЕ РАСПРОСТРАНЕННЫЕ КИБЕРАТАКИ Несмотря на появление сложных вредоносных инструментов, наподобие Industroyer, около 70% кибератак на энергообъекты построено на социальной инженерии, говорят в ESET Russia «Наиболее распространенный сценарий — письма с вредоносными вложениями и ссылками. Такие письма получает любая организация, в том числе и организации энергетического сектора»,— поясняет Виталий Земских. Стандартные меры защиты, по его словам,— комплексные решения для безопасности, включая продукты для защиты почтовых серверов, обучение персонала. В ЛК согласны, что самые распространенные атаки — фишинг с целью разведки и кражи данных, неспециализированное вредоносное ПО, включая шифровальщики и вымогатели, нарушения правил эксплуатации персоналом, приводящие к другим инцидентам.

В этом году две из трех эпидемий вирусов-шифровальщиков, WannaCry и NotPetya, серьезно затронули энергетический сектор, напоминает замдиректора центра информационной безопасности компании «Инфосистемы Джет» Андрей Янкин. «Если говорить о борьбе с такого рода проблемами, то здесь помогают в первую очередь самые базовые меры ИБ, которые можно отнести к „цифровой гигиене“: управление уязвимостями, обновление систем, жесткое разграничение доступа как на сетевом, так и на логическом уровне, контроль работы подрядчиков, обучение работников основам ИБ. Если же говорить о более изощренных хакерских атаках, то тут меры защиты, конечно же, сложнее, но базовая защита и порядок в IT очень помогают и здесь»,— поясняет господин Янкин.

Сложность объектов энергетического сектора, их существенная распределенность предполагает наличие многих уровней, эшелонов и методов защиты, отмечает техдиректор компании Check Point Software Technologies Никита Дуров. «Так, в SCADA-системах крупных предприятий существуют три сегмента, которым необходима защита. Первый сегмент отвечает за диспетчерское управление, для его защиты можно использовать уже имеющиеся в организации решения: системы обнаружения вторжения, антивирусы, межсетевые экраны. Далее следует сегмент контроллеров, отвечающих за технологический процесс, а также сегмент управляющих устройств, например, датчиков или переключателей. К защите каждого сегмента необходим особый подход, и только комплексная работа будет иметь долгосрочный эффект»,— говорит он.

Самой громкой атакой на энергетические объекты господин Дуров называет Stuxnet, атаковавший в 2010 году ядерные объекты Ирана: именно с него началась эра применения вредоносного кибероружия в масштабах целых государств В рамках такой атаки злоумышленники перехватывают управление энергоблоками, что может привести к катастрофе. «Для защиты от этой угрозы применяется изоляция сетей управления автоматизированной системы управления технологическим процессом (АСУ ТП) от корпоративных сетей с помощью дата-диодов»,— пояснил BG руководитель направления информационной безопасности компании «Системный софт» Яков Гродзенский.

Респонденты исследования EY из сферы энергетики отмечают следующие топ-5 киберугроз, реализация которых привела к значимым последствиям за 2017 год: фишинг, зловредное программное обеспечение, атаки с использованием уязвимостей нулевого дня, мошенничество, шпионаж. «Задача управления рисками и противодействия угрозам кибербезопасности является комплексной и требует детальной проработки на многих уровнях: это и выстраивание механизмов кросс-функционального взаимодействия между структурными подразделениями, и выстраивание процессов управления кибербезопасностью, и внедрение системы управления киберустойчивостью, и выбор актуальных средств защиты, работа которых фокусируется не только на устранении последствий, но и на механизмах выявления кибератак на ранних стадиях их развития»,— поясняет господин Самодаев.

Северо-Западные энергетики берут на вооружение технологии защиты против кибератак. Так, в ЛК рассказали BG, что использовали специализированное решение для защиты IT-инфраструктуры подстанции в Вологодской области филиала ПАО «МРСК Северо-Запада». «В ходе подготовки к внедрению специалисты по кибербезопасности проверили в действии защиту ключевых узлов IT-инфраструктуры подстанции и исследовали технологическую сеть на предмет потенциальных уязвимостей»,— рассказал Антон Шипулин.

В ПАО «Ленэнерго» сообщили BG, что к чемпионату мира по футболу 2018 года информационная безопасность усилена. «Учитывая значительный рост количества киберугроз, в компании внедряются лучшие решения ведущих разработчиков, предпочтение отдается российским вендорам. При этом и существующие технические решения позволяют предотвратить негативное влияние кибератак на работу объектов „Ленэнерго“»,— сказали в пресс-службе компании. Там отметили, что успешно реализованных атак на объекты «Ленэнерго» не было.

ПОД НАДЗОРОМ ГОСУДАРСТВА Требования к ИБ в России будут ужесточаться. «С 1 января 2018 года вступает в силу 187-ФЗ „О безопасности критической информационной инфраструктуры РФ“. И там отношение к регулированию области информационной безопасности строже: вводится уголовная ответственность как за попытки несанкционированного доступа в информационную систему, так и за нарушение правил эксплуатации IT на предприятиях, если это повлекло за собой какие-либо инциденты»,— напоминает старший менеджер по маркетингу компании «Код безопасности» Павел Коростелев.

В энергосекторе тенденцию на усиление требований к ИБ еще сильнее «разогнал» скандал с поставками турбин Siemens, так как добавились риски, связанные с политическими санкциями, указывает председатель совета директоров «СёрчИнформ» Лев Матвеев. «Летом замминистра энергетики Андрей Черезов подчеркнул необходимость усилить информационную безопасность на объектах электроэнергетики, так как проведенная оценка рисков показала, что при передаче и хранении данных за рубеж возможно удаленное управление энергетическим оборудованием вплоть до его отключения. Тогда же Минэнерго РФ подготовило и разместило проект нормативного правового акта, содержащего правила по предотвращению внешних и внутренних угроз информационной безопасности на объектах ТЭК. Конечно, регулирование существовало и раньше, однако работали по большей части общие требования, не отраслевые»,— отмечает господин Матвеев.

Директор центра компетенций по информационной безопасности компании «Техносерв» Сергей Терехов отмечает, что выбор технологий и их поставщиков осуществляется с учетом требований действующего законодательства, но на усмотрение каждой энергетической компании. «Предъявлялись требования, как к сертификации средств защиты, так и к соответствию SCADA и оборудования требованиям информационной безопасности, в том числе в части контроля отсутствия недекларированных возможностей. Новые правила регулирования наверняка помогут навести порядок, в особенности в части правил информационной безопасности в отношении удаленного доступа к энергообъектам»,— говорит господин Терехов. ■