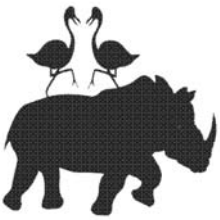

Еще пару десятилетий назад взлом электронной почты требовал серьезных навыков программирования. Сегодня реальностью становятся молниеносные и анонимные атаки на банковские системы, подключенную к интернету бытовую технику и медицинское оборудование. Все чаще звучит термин *кибервойна*. Провозвестником новой эры стал вирус *Stuxnet*, в 2010 г. поразивший иранские центрифуги для обогащения урана и отбросивший ядерную программу страны на пару лет назад. Из проблем *второго эшелона* вопросы кибербезопасности переходят в категорию ПОВТОРНО, СРОЧНО.

О защите критической энергетической инфраструктуры от киберугроз, существующих пробелах в законодательстве и планах по их ликвидации главному редактору *Индекса Безопасности* О. Мостинской рассказал заместитель министра энергетики Российской Федерации Ю. Сентюрин.

Юрий Сентюрин:

«МЫ НЕ МОЖЕМ НЕ ВОСПРИНИМАТЬ ВСЕРЬЕЗ УТВЕРЖДЕНИЯ КОЛЛЕГ, КОТОРЫЕ ГОВОРЯТ О ПРИЗНАКАХ БОЕВЫХ ДЕЙСТВИЙ В КИБЕРПРОСТРАНСТВЕ»

— Уровень информатизации объектов ТЭК очень высок и постоянно растет. Возможны ли киберинциденты на объектах критической энергетической инфраструктуры, которые бы привели к серьезным авариям, аналогичным по масштабу аварии на Саяно-Шушенской ГЭС, — внеплановым сбросам воды или серьезным перебоям с энергоснабжением? Случались ли уже такие инциденты?

— По моему личному мнению, такого рода воздействия на работающую ТЭКовскую систему возможны. В этих вопросах министерство ориентируется на информацию и установки, которые мы получаем от профильных ведомств и организаций.

Очевидно, что реальная опасность в киберпространстве существует и нарастает. Безусловно, это является предметом обсуждения на специальных площадках. К слову, помимо отечественных экспертов такими же проблемами занимаются наши зарубежные партнеры. И мы не можем не воспринимать всерьез утверждения коллег, которые говорят о признаках *боевых действий* в киберпространстве. Это, безусловно, алармистская терминология, но не учитывать эти мнения, сбрасывать их со счетов нельзя.

Возможно ли эти вещи увидеть на конкретных примерах? К сожалению, да. Потому как управление производственным процессом на объектах критической топливно-энергетической инфраструктуры обеспечивается с помощью информационно-коммуникационных систем. Хотя в большинстве своем они работают в автономном режиме, без соприкосновения с глобальным киберпространством не обойтись. Есть примеры, когда пуски и остановы энергоблоков — а это ключевой элемент энергетического комплекса — имели место не с пульта оператора, размещающегося на энергообъекте, а из удаленных центров доступа. Понятно, что на этих коммуникационных линиях возможны разного рода несанкционированные действия.

С учетом нынешней ситуации в мире целесообразно действовать в режиме перестраховки. Такой подход позволяет чувствовать себя безопаснее, надежнее обеспечивать потребителей — промышленность, домохозяйства. Нельзя пренебрегать необходимостью повышать защищенность наших информационно-телекоммуникационных систем и информационных массивов от разного рода недружественных системных воздействий. Мы это понимаем и соответствующие действия предпринимаем.

Отмечу, что в киберпространстве имеют место и проявления киберхулиганства. Вреда от них не меньше. Армия профессиональных взломщиков, хакеров, которые орудуют в киберпространстве, далеко не всегда руководствуясь чистыми и благородными целями, разрастается. Информация об этом идет из самых разных источников, в том числе от известной *Лаборатории Касперского*. Свою задачу мы видим в том, чтобы обеспечить глобальную защиту, особенно в свете усложняющихся межгосударственных отношений.

Мы видим, какие угрозы и вызовы стоят перед нами. Вопрос в том, как на эти вызовы реагировать, какими силами и средствами. Энергетики понимают, что объекты ТЭК являются приоритетными, критически значимыми, обеспечивающими основы жизнедеятельности современной цивилизации. Логично, что эти объекты и их информационно-коммуникационные системы нуждаются в защите. Поэтому в законе, направленном на обеспечение безопасности объектов ТЭК, есть специальная статья по безопасности информационных систем. Статья — это акцент на проблеме. Задача соответствующих министерств и ведомств — подкрепить этот акцент практическими действиями.

— Вы упомянули 256-й закон и его статью 11. В ней действительно говорится об обеспечении безопасности информационных систем объектов ТЭК, но не содержится никаких конкретных требований. При этом, насколько я знаю, еще в 2013 г. был подготовлен проект закона о безопасности критической информационной инфраструктуры, который получил неплохую оценку со стороны экспертного сообщества. В нем есть ряд весомых досто-

инств: прописаны основные определения, зоны ответственности. Однако он до сих пор не принят. Почему и какие у него перспективы?

— Этот законопроект готовился не по линии Минэнерго России. У каждого ведомства своя зона ответственности. Есть государственные органы, которые по своему профилю отвечают за это направление работы. Мы были причастны к этому документу как соисполнители и последовательно выступали в его поддержку. Параллельно с разработкой этого концептуального документа мы в рамках ведомственных полномочий работали над обеспечением информационной безопасности наших объектов.

В 2013 г. мы вышли с предложением внести изменения в ФЗ 256 *О безопасности объектов ТЭК*. Этот закон был принят в середине 2011 г., начал применяться в полном объеме с 1 января 2012 г. Концептуально ответственность за обеспечение безопасности закон возлагает на собственников объектов ТЭК при том понимании, что ответственность государства состоит в противодействии экстремизму, терроризму, обеспечении глобальной безопасности. Возлагая ответственность на корпоративный сектор, государство устанавливает требования, стандарты, ниже которых нельзя *опускаться* в выстраивании систем защиты.

Таков общий подход. Однако если по направлениями физической защиты, по вопросам привлечения персонала, который отвечает за обеспечение безопасности, правила и требования были подробно прописаны, то в сфере защиты информационно-коммуникационных систем был просто сделан акцент и было обозначено, что ответственность лежит на бизнесе. *Централизованных* правил и требований, устанавливаемых государством, предложено не было. Поэтому в 2013 г. мы предложили внести изменения в ФЗ 256, чтобы собственники, несущие всю полноту ответственности за обеспечение безопасности, имели ориентиры для практической работы.

Этот замысел не был реализован в полном объеме, в том числе из-за опасений наших партнеров из корпоративного сектора по поводу *завышения* требований, что могло, по их мнению, привести к существенному возрастанию затрат, *перестройке* технической части, поскольку сегодня всем очевидно, что в этой работе нужно ориентироваться на отечественные разработки, элементную базу и технику.

Вместе с тем, весьма непросто, оказавшись перед столь широкой гаммой вызовов, как снижающаяся стоимость энергоресурсов на мировом рынке, односторонние санкции, ограничение доступа к передовым технологиям, пойти на серьезные затраты в целях решения вопросов, которые еще недавно воспринимались как задачи сопутствующего характера. Поэтому вопрос разумного баланса, золотой середины является принципиально важным.

Поясню на примере: в сентябре 2015 г. вышло постановление правительства России, устанавливающее правила обеспечения безопасности линейных объектов ТЭК. Этот документ готовился довольно долго как раз по тем причинам, о которых я говорил: страна очень большая, миллионы километров электрических воздушных линий и десятки тысяч километров трубопроводов. Их надежная защита безусловно требует больших расходов. Поэтому выходу документа предшествовала

интенсивная дискуссия, позволившая найти взвешенный компромисс. Государство понимает, что сегодня ввести *сверхзатратные* требования, конечно, нельзя.

Аналогичный подход принят за основу в работе по защите от киберопасности. Есть понимание, что угроза реальна, и именно государство должно сформулировать универсальные подходы к обеспечению безопасности на уровне отдельных компаний.

Пока не приняты изменения в ст. 11 ФЗ 256, мы работаем на уровне ведомственных нормативных актов. Функционирует созданная приказом министерства рабочая группа по противодействию терроризму в ТЭК. Это межведомственный орган, в состав которого помимо министерских работников и руководителей службы безопасности компаний ТЭК входят представители МВД, ФСБ, Национального антитеррористического комитета, министерства юстиции, МЧС — в общем, все профильные специалисты. На этой площадке мы и прорабатываем такого рода вопросы.

В частности, изучены специфика организации защиты информационных систем в компаниях — лидерах рынка. Это компании электроэнергетического, нефтегазового, угольного профиля. Проведен обмен мнениями и опытом, мы посмотрели, как степень защищенности оценивается специалистами эксплуатирующих организаций. Отмечу, что универсальных подходов нет. В итоге специалисты, изучив весь этот материал, пришли к выводу о необходимости унификации требований, в т. ч. в связи с запуском механизма государственного контроля (надзора) за обеспечением безопасности объектов ТЭК. Эта функция закреплена за МВД России. Предусмотрена система плановых и внеплановых проверок. Возникает вопрос: чем проверяющая инстанция будет руководствоваться, *тестируя* систему защиты информационно-коммуникационного блока? Естественно, пока придерживаемся требований приказа ФСТЭК № 31, притом что, по мнению специалистов, в этом документе, несмотря на его универсальность, в полном объеме специфика ТЭКовских объектов не учтена.

— Есть еще одна проблема: приказ ФСТЭК не опирается ни на один федеральный закон, поэтому его юридическая сила не очевидна.

— Именно поэтому считаем, что ст. 11 должна быть дополнена полномочиями правительства Российской Федерации устанавливать подобного рода правила и требования.

При этом важно учесть передовой опыт и все имеющиеся наработки, не забывая о необходимости сбалансированного подхода, чтобы, заботясь о защите информационных систем, мы не набросили удавку на бизнес в виде чрезмерных расходов. Простого решения тут быть не может. Безусловно, потребуется переходный период, время на адаптацию, время на то, чтобы развернуть производство соответствующих мировым стандартам отечественных аналогов.

В этом направлении мы сейчас планово движемся. Работаем через механизм специально созданной при вышеупомянутой рабочей группе министерства секции, в состав которой вошли представители ключевых компаний ТЭК, коллеги из ФСТЭК и других специализированных организаций, как государственных, так

и частных. Мы рассчитываем к концу первого квартала 2016 г. получить базовый материал, который вынесем на широкое общественное обсуждение.

— Работа предстоит довольно масштабная. При этом есть опыт других стран, других отраслей. Ведется ли международное, межведомственное сотрудничество? Большой опыт обеспечения кибербезопасности есть у атомной отрасли, у* Росатома*, МАГАТЭ, которое выпустило уже немало регламентов по кибербезопасности. В этом году состоялась первая* Конференция МАГАТЭ по компьютерной безопасности в ядерном мире*. Есть ли планы использовать опыт коллег?

— Безусловно, несмотря на специфику производственных процессов в ТЭКе, информационно-коммуникационные системы, используемые в отрасли, достаточно универсальны. В основе нашей работы — изучение опыта передовых компаний, в том числе работающих в атомной отрасли. Что касается международного опыта — секции поставлена задача изучить все тематические публикации, в том числе документы МАГАТЭ.

Естественно, не вся информация находится в режиме свободного доступа, такова специфика темы. Однако изобретать велосипед не собираемся, будем опираться на передовой опыт.

— Сегодня за промышленную и информационную безопасность отвечают разные ведомства. Что, если произойдет киберинцидент с серьезными последствиями? В их ликвидации будут задействованы и ФСТЭК, и ФСБ, и МВД, и Минэнерго. Как будет делиться ответственность? Существуют ли механизмы координации?

— Затронут очень важный вопрос. Мы работаем параллельно — я упоминал это, когда рассказывал о проекте закона, который разрабатывают коллеги из соседних структур. Мы пытаемся решить проблему через механизм межведомственной рабочей группы, привлекая туда всех, кто причастен к этой работе, чтобы избежать дублирования норм и требований.

Наша задача — безусловно, привести все к единому знаменателю. Упомянутая секция столкнулась с проблемой стыковки норм промышленной, информационной и прочих видов безопасности. В этой работе нам очень помогает, к примеру, помимо упомянутых структур, Межведомственная рабочая группа Совета Безопасности России по информационной безопасности. На этой площадке мы получаем материал установочного характера, пытаемся потом к нему пристыковать отраслевую специфику и вносим предложения, которые не противоречат общим установкам.

— Есть ли планы по проведению учений для отработки координации действий различных ведомств в случае чрезвычайных ситуаций, вызванных киберинцидентами?

— Такие задумки есть. Подобного рода учения — требования жизни. Приведу пример: в начале ноября текущего года после террористических атак во Франции мы провели всероссийское селекторное совещание, поставили задачу организовать тренировки корпоративного уровня, проверить надежность работы всех наших

коммуникационных систем и связи. При возникновении сложной ситуации — будь то ЧС, техногенная авария или противоправное вмешательство в деятельность отраслевого субъекта — необходима система коллективных контрмер. Поэтому все системы взаимодействия находятся в повышенной готовности. Специального акцента на том сценарии учений, о котором вы говорите, мы не делаем. Одна из причин — подобного рода тренировки проводятся по инициативе профильных организаций, комплексно отвечающих за вопросы противодействия экстремизму в силу специального закона. По нашей информации, такие планы есть.

Вопросы киберопасности обсуждаются все шире. Серьезный анализ проводился во время подготовки и проведения Олимпийских и Паралимпийских игр в Сочи. Тогда была развернута целая система контроля за киберпространством, фиксировались киберпосягательства, приняты своевременные меры. Эти события дали толчок к активизации наших усилий по совершенствованию 11-й статьи и по созданию специальной секции министерской рабочей группы по противодействию терроризму. Процесс пошел.