# Информационная безопасность в электроэнергетике
## Отраслевые нюансы

**Денис ПРОХОРОВ**,
менеджер по работе
с заказчиками,
ОАО «ЭЛВИС-ПЛЮС»

**Андрей КОНДРАТЕНКО**,
начальник отдела ИБ
Департамента обеспечения
безопасности, ОАО «СО ЕЭС»

**Сегмент электроэнергетики всегда был достаточно крупным на рынке информационной безопасности (ИБ), что раньше обусловливалось прежде всего повышенным вниманием руководства РАО ЕЭС к данному вопросу и трансляцией своей позиции директивным методом подведомственным предприятиям. На стыке 2008–2009 гг. отрасль подверглась влиянию сразу нескольких внешних факторов, в дальнейшем изменивших основные драйверы ИБ в организациях. И что самое интересное, мировой финансовый кризис оказался далеко не на первом месте по значимости.**

Первым таким фактором стала реорганизация РАО ЕЭС. В первую очередь реорганизация повлияла на децентрализацию центров принятия решений. Раньше РАО ЕЭС выступало в качестве основного отраслевого регулятора, который формировал общее понимание концепции ИБ в энергетике и имел все рычаги воздействия для достижения ее реализации. Теперь же единственным регулятором осталось Минэнерго, с гораздо меньшей степенью самомотивации к решению этих вопросов и с большей инертностью, как любое государственное ведомство. Поэтому центры формирования стратегии ИБ постепенно передвинулись на места и таким образом, с одной стороны, стали «ближе к народу», а с другой – привели к сильному разночтению в понимании проблем обеспечения ИБ в отрасли.

Другим фактором явился Закон № 152-ФЗ «О персональных данных», точнее, даже не сам закон, принятый еще в 2006 г., а сроки приведения информационных систем персональных данных в соответствие с ним. Как ни странно, но компании в секторе электроэнергетики, хотя и обрабатывающие персональные данные преимущественно только собственных работников, тем не менее быстрее всех среагировали на выполнение требований закона, не дожидаясь переносов сроков, изменений нормативных документов, и вообще оказались в стороне от жарких дискуссий по этим вопросам. Это связано с тем, что большинство организаций в электроэнергетике являются компаниями публичными, акции которых котируются на биржах и для которых вопросы любого соответствия требованиям регуляторов могут отражаться на стоимости их акций. Как следствие, компании энергетического сектора проявили высокую сознательность в выполнении требований по приведению своих информационных систем в соответствие с требованиями Закона «О персональных данных». Дополнительным стимулом развития ИБ в энергетических компаниях можно считать Федеральный закон № 224-ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации», который предъявляет требования к порядку использования и защиты инсайдерской информации.

Еще один важный фактор – развитие угроз в сфере безопасности критических инфраструктур. В этой сфере произошли сразу несколько событий, как внутренних, так и международного масштаба. Это и страшная трагедия на Саяно-Шушенской ГЭС, и обнаружение вредоносного кода stuxnet на Бушерской АЭС в Иране и т. д. Анализ динамики показателей с 2007 г. отчета GlobalRisks, который ежегодно готовится в рамках Всемирного экономического форума, свидетельствует о том, что риск безопасности критических инфраструктур занимает одно из самых высоких мест по шкале «критичность последствий». Все это стало причиной того, что в Минэнерго приступили к формированию требований по обеспечению безопасности АСУ ТП, и в достаточно короткие сроки был подготовлен Федеральный закон от 21 июля 2011 г. № 256-ФЗ «О безопасности объектов топливно-энергетического комплекса», ст. 11 которого напрямую обязывает организации ТЭК создавать системы защиты информации. А Федеральным законом № 257-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части обеспечения безопасности объектов топливно-энергетического комплекса» была введена дополнительная ответственность.

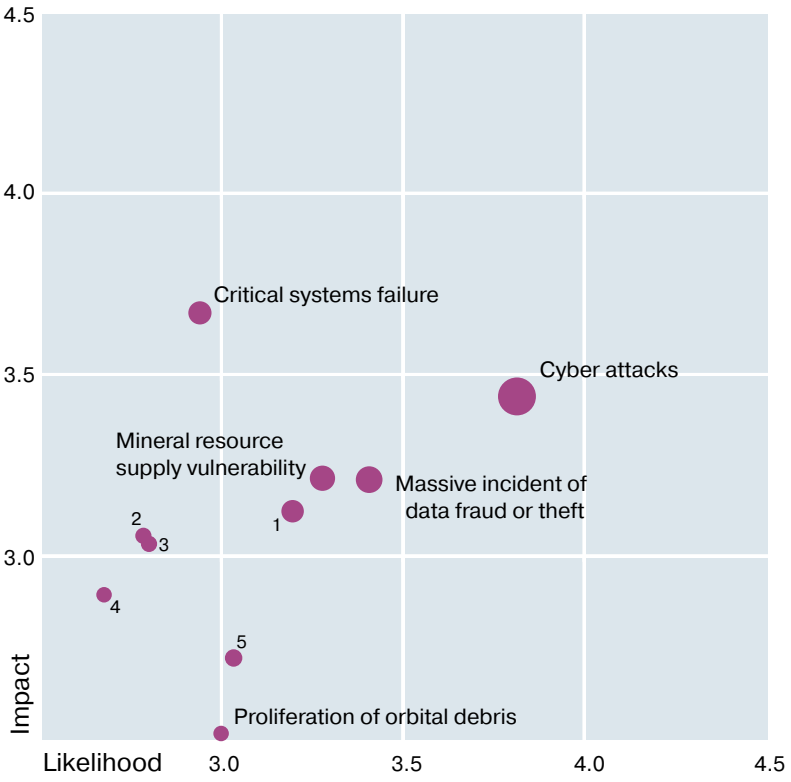


Рисунок. Карта технологических рисков из отчета «GlobalRisks 2012. Seventhedition» Международного экономического форума

*Источник: World Economic Forum*

Таким образом, основным движущим фактором развития проектов ИБ на предприятиях электроэнергетики является необходимость обеспечения безопасности:

- информационных систем персональных данных;
- информационных систем критических инфраструктур;
- инсайдерской информации.

Выполнение этих требований и определяет выбор основных решений ИБ, внедряемых в проектах ИБ предприятий электроэнергетики. Вполне логично, что самой массовой услугой стал аудит. С одной стороны, без аудита достаточно сложно проверить полноту реализации требований закона «О персональных данных», с другой – рекомендации о проведении оценки актуальных угроз были сформулированы рабочей группой Минэнерго в рамках выработки мер по повышению безопасности критических инфраструктур.

> Все информационные системы энергетических компаний направлены на обеспечение основной задачи – бесперебойной генерации и своевременной доставки электроэнергии потребителям.

Все информационные системы энергетических компаний направлены на обеспечение основной задачи – бесперебойной генерации и своевременной доставки электроэнергии потребителям. Поэтому главная задача ИБ – обеспечение в первую очередь ДОСТУПНОСТИ информации. Вопросы целостности и конфиденциальности вторичны, ничто не должно воспрепятствовать технологическому процессу. Все перечисленное и обусловливает главные особенности ИБ в отрасли, начиная от выстраивания концепции и заканчивая политикой использования конкретных средств защиты информации. На уровне концепции, в частности, осуществляется обязательное сегментирование ИС с выделением АСУ ТП в отдельный сегмент. На уровне политик использования СЗИ можно привести такой пример: все средства по возможности настраиваются на работу в режиме мониторинга, чтобы исключить любое самостоятельное блокирование каких-либо функций. Это касается и средств антивирусной защиты, и средств предотвращения вторжений, и других средств защиты информации, причем даже в системах электронного документооборота, не говоря

уже об ИС, связанных с технологическими процессами.

Если говорить об обеспечении ИБ непосредственно самих АСУ ТП, то необходимо отметить, что, несмотря на важность данного вопроса, внимания ему уделялось меньше, чем безопасности тех же ИСПДн. Связано это, во-первых, с отсутствием контролирующей функции со стороны государственных регуляторов, во-вторых, с тем, что ИБ АСУ ТП всегда рассматривается в комплексе общих мер по обеспечению безопасности критически важных объектов, в котором гораздо больше внимания уделяется физической и технической безопасности. Отчасти это обусловлено и тем фактом, что реализации угроз именно информационной безопасности на критических объектах в нашей стране пока, к счастью, не происходило и риски являются невысокими по вероятности, хотя крайне критичными по последствиям. Точных данных по оценке ИБ-рисков для критических объектов нет, но вряд ли они превышают показатели общих рисков разрушения критических инфраструктур (см. рисунок).

> Решение проблемы управления рисками ИБ в компаниях энергетического сектора пока находится в начальной стадии развития, хотя уже достаточно активного.

Проводимые по заказу разных энергетических компаний многочисленные тесты на проникновение с целью анализа защищенности информационных систем действительно показали наличие серьезных уязвимостей в АСУ ТП, позволяющих реализовать угрозы информационной безопасности. Поэтому данная тема активно развивается, особенно в свете выхода федеральных законов № 256-ФЗ и № 257-ФЗ, а также возрастающей активности Минэнерго в этом направлении. Однако решение проблемы управления рисками ИБ в компаниях энергетического сектора пока находится в начальной стадии развития, хотя уже достаточно активного. Усиление интереса связано с тем, что риски ИБ стали попадать в категорию серьезных бизнес-рисков и заметны подразделениям, отвечающим за управление ими. Хорошим примером может служить ситуация с выполнением требований № 152-ФЗ. Нередко решающую помощь в обосновании бюджетов на мероприятия по приведению ИСПДн в соответствие оказывали юридические службы заказчика, являющиеся обычно главным препятствием. Никакого чуда в этом нет, поскольку, как отмечалось выше, самым главным требованием является ДОСТУПНОСТЬ, и малейший риск приостановки основной деятельности организации в результате проверок государственными регуляторами был воспринят юристами как недопустимый. Вообще оценка информационных рисков – достаточно перспективная тема для ИБ проектов в организациях электроэнергетики.

Еще одна важная особенность, которая накладывает свой отпечаток на проекты ИБ в электроэнергетике, – большая территориальная распределенность информационных систем энергетических компаний с необходимостью реализации централизованной политики безопасности. По этой причине реализуется большое количество проектов по построению подсистем централизованного управления теми или иными сегментами системы обеспечения информационной безопасности (СОИБ): аутентификацией и доступом пользователей, ключевой инфраструктурой, DLP-системами и сегментами сетевой безопасности.

Теперь что касается облачных вычислений. В компаниях электроэнергетики практически не проявляется интерес даже к частным облакам, не говоря уже о публичных, что вполне объяснимо, учитывая важность обеспечения ДОСТУПНОСТИ информационных ресурсов. На этом фоне проблема ИБ в облачных решениях соответственно не поднимается.

Ну и в заключение – о влиянии мирового финансового кризиса. Можно сказать, что он практически не отразился на финансировании ИБ-проектов в энергетических компаниях. И если у каких-то заказчиков и происходило урезание или, наоборот, увеличение бюджетов на информационную безопасность, связано это было исключительно с внутренними процессами в организации. В принципе, на предприятиях нет единой модели бюджетирования и формирования политики информационной безопасности только службами ИТ или только службами безопасности. В разных компаниях эти функции могут «плавать» от одной к другой, как и управление бюджетами. Однако в свете последних тенденций повышения безопасности на предприятиях критических инфраструктур идет планомерная работа по концентрации вопросов информационной безопасности в отдельно выделенных структурах. К примеру, даже когда отдел информационной безопасности входит в структуру ИТ-службы, политику ИБ определяет заместитель директора по безопасности, должность которого постепенно и повсеместно начинают вводить во многих компаниях и филиалах.

Таким образом, тренд разделения ИБ и ИТ наблюдается во многих компаниях энергетического сектора.

Подводя итоги, можно смело сказать, что сегмент электроэнергетики еще долго будет одним из самых интересных и «лакомых» с точки зрения внедрения решений информационной безопасности. Основанием этому будут служить неутешительные прогнозы по возрастанию рисков для объектов критических инфраструктур, а также возникающие тренды усиления государственного регулирования вопросов безопасности на подобных объектах. ■