СЦЕНАРНЫЙ ПОДХОД К ОПРЕДЕЛЕНИЮ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ

Гаськова Д.А.
Массель А.Г.
Институт систем энергетики им. Л.А. Мелентьева СО РАН, г. Иркутск, ул. Лермонтова, д.130, 664033
gaskovada@gmail.com

Введение

Энергетика проникла во все сферы жизнедеятельности современного общества, а энергетическая безопасность (ЭБ) рассматривается как составляющая национальной безопасности страны. Среди угроз ЭБ выделяют тактические и стратегические угрозы [1]. Угрозы ЭБ систематизируются в пять основных групп: экономические, социально-политические, техногенные, природные и управленческо-правовые. Этот перечень угроз был расширен угрозами кибербезопасности [2], реализация которых может спровоцировать серьезнейшие чрезвычайные ситуации в энергетике, которые могут повлечь снижение возможностей обеспечения энергоресурсами потребителей.

Стремительное распространение компьютерной среды, развитие информационных технологий и тенденция перехода к интеллектуальной энергетике делают киберугрозы одной из важнейших тактических и стратегических угроз ЭБ.

В исследованиях критических инфраструктур, энергетику выделяют как одну из основных частей гражданской инфраструктуры, выведение из строя или уничтожение которой может привести к ущербу, сопоставимому с ударами, наносимыми по вооруженным силам [3].

Предлагается сценарный подход к анализу возможных критических ситуаций в энергетическом секторе как инструмент стратегического планирования, направленного на выявление критически важных объектов (КВО).

Определение КВО

Критически важными объектами называют ключевые объекты (или их совокупности) соответствующих инфраструктур, воздействие на которые может оказать наиболее негативный эффект на отрасль экономики, ключевой ресурс или всю инфраструктуру.

Корректное определение КВО в энергетике позволит снизить риски финансовых потерь при повреждении или уничтожении энергетических объектов и будет способствовать бесперебойному получению энергетического продукта на стороне потребителя.

Критически важные объекты предлагается определять исходя из рисков наступления экстремальных ситуаций, вызванной нарушением кибернетической безопасности критической информационной инфраструктуры (КИИ) энергетических объектов. Для определения КИИ разрабатывается риск-ориентированный подход, основанный на методах определения уязвимостей информационно-технологической системы объекта, сценариотехника для выявления КС от реализации киберугроз и методах искусственного интеллекта. На основе анализа возможных экстремальных ситуаций путем ранжирования предлагается выявлять КВО.

Сценарный подход

Сценарий представляет совокупность цепочки угроз ЭБ, которые с определенной вероятностью могут наступить при реализации киберугрозы, условий наступления того или иного негативного события, а также последствий, приводящих к ущербу, называемой экстремальной ситуацией.

Под экстремальными ситуациями (ЭкС) в энергетике понимают как чрезвычайные, так и критические ситуации. Под критическими ситуациями понимаются ситуации, когда возникают угрозы бесперебойному функционированию технических объектов и объектов обеспечения жизнедеятельности и/или угрозы жизни или здоровью, как отдельных людей, так и социальных (профессиональных) групп [4].

На рисунке 1 представлены компоненты сценария. Энергетические объекты содержат активы, представляющие собой программно-аппаратные составляющие информационно-технологической системы, которые могут содержать уязвимости разной степени значимости. Уязвимости могут быть использованы злоумышленником, т.е. реализованы киберугрозы в виде кибератаки или вследствие ошибки сотрудника как киберхалатность (вызванная низкой компьютерной грамотностью или пренебрежением инструкциями).

Рис.1. Онтология сценария реализации угроз

Основным компонентом сценария является событие, представляющее собой реализованную угрозу по отношению к активу энергетического

объекта, приводящую к негативным последствиям. Формально событие (E) можно представить, как:

$$E = \{A_i, C_i, N_i\},$$

где A – актив, C – последствия, N – условия.

Последствия (C), представленные в сценарии, далее ранжируются в соответствии с вероятностью их наступления и критериями оценки, в качестве которых могут выступать такие категории как финансовая оценка, экологические оценки, качество жизни населения и др.

$$C = \{D, K\},$$

где D – ущерб, K – критерии оценки.

С использованием шкалы: «норма», «предкризис» — критическая ситуация, «кризис» — чрезвычайная ситуация [4] — производится оценка сценария и далее анализируются риски наступления критической ситуации. Риски определяются тройкой:

$$R = \{T, V, D\},$$

где T – угрозы, V – уязвимости, D – ущерб при реализации угрозы.

Ущерб определяется для каждого последствия, как экономическая эффективность сценария. Под экономической эффективностью понимается соотношение между полученными оценками рисков наступления критической ситуации, выраженными в денежных единицах, и стоимостью выбранных контрмер, с учетом критериев оценки.

Степень риска устанавливается экспертом от допустимого до критического. На основе ранжирования критических рисков возникновения критической ситуации выявляются КВО с наибольшим ущербом для территории, региона или в масштабах страны.

Для поддержки принятия решений по построению сценариев возможных критических ситуаций экспертом-энергетиком предлагается разработать программный инструмент на основе Байесовских сетей доверия.

Байесовские сети доверия

Байесовская сеть – это графическая модель вероятностных и причинно-следственных отношений между наборами переменных, представляющая собой направленный ациклический граф, вершины которого представляют переменные, а ребра показывают условные зависимости между переменными [5].

Ранее Байесовские сети применялись для анализа угроз энергетической безопасности [6]. Применение Байесовских сетей как инструмента реализации сценарного подхода, рассчитанного на стратегическое планирование, позволит строить модели критических ситуаций с использованием байесовских вероятностей при введении числовых значений на основе знаний и опыта эксперта или частотных вероятностей при наличии статистических данных, зачастую отсутствующих в свободном доступе.

Байесовские сети позволят реализовать анализ угроз, охватывающий широкий круг параметров и полный объем угроз для определенной ЭкС, с возможностью оценки конкретных узких мест в зависимости от степени детализации анализа информационно-технологической системы энергетического объекта. При формировании сценариев реализации угроз нарушителем важной составляющей является исследование возможных последствий реализации неблагоприятных событий, при которых, задавая свидетельство для одного узла, производится оценка значений его потомков (последствий события)[6].

Заключение

Предложен подход к первичному выявлению КВО на основе построения сценариев ЭкС ситуаций в энергетике с применением анализа критической информационной инфраструктуры при реализации кибератаки на энергетический объект с использованием вероятностного моделирования (на основе Байесовских сетей доверия).

Данный подход позволяет моделировать ЭкС для дальнейшего анализа рисков их возникновения и выявления КВО.

Список использованных источников

1. Энергетическая безопасность России: проблемы и пути решения / Н.И. Пяткова, В.И. Рабчук, С.М. Сендеров, М.Б. Чельцов. Отв. ред. Воропай Н.И. – Новосибирск: Изд-во СО РАН, 2011. – 211 с.
2. Массель Л.В., Воропай Н.И., Сендеров С.М., Массел А.Г. Кибербезопасность как одна из стратегических угроз энергетической безопасности // Вопросы кибербезопасности. №4 (17). 2016. – С 2-10.
3. Кондратьев А. Современные тенденции в исследовании критической инфраструктуры в зарубежных странах / Зарубежное военное обозрение. - 2012. - № 1. - С. 19-30.
4. Массель Л.В., Массель А.Г. Технологии и инструментальные средства интеллектуальной поддержки принятия решений в экстремальных ситуациях в энергетике // Вычислительные технологии. 2013. Т. 18. № S1. С. 37-44.
5. D. Heckerman. A Tutorial on Learning with Bayesian Networks // Technical Report MSR-TR-95-06, Microsoft Research, March, 1995, 57 p.
6. Массель Л.В., Пяткова Е.В. Применение байесовских сетей доверия для интеллектуальной поддержки исследований проблем энергетической безопасности. – Вестник ИрГТУ. – №2. – 2012. – С. 8-13.