8. Barendregt H., Dekkers W., Statman R. Lambda calculus with types. – Cambridge University Press, 2013.
9. Вольфенгаген В. Э. Методы и средства вычислений с объектами. Аппликативные вычислительные системы. — М: JurInfoR Ltd., АО «Центр ЮрИнфоР», 2004. – XVI+789с.
10. Siek J., Thiemann P., Wadler P. Blame and coercion: together again for the first time //ACM SIGPLAN Notices. – ACM, 2015. – Т. 50. – №. 6. – С. 425-435.
11. Abadi M. et al. Dynamic typing in a statically typed language //ACM transactions on programming languages and systems (TOPLAS). – 1991. – Т. 13. – №. 2. – С. 237-268.
12. Henglein F. Dynamic typing: Syntax and proof theory //Science of Computer Programming. – 1994. – Т. 22. – №. 3. – С. 197-230.
13. Siek J. G., Taha W. Gradual typing for functional languages //Scheme and Functional Programming Workshop. – 2006. – Т. 6. – С. 81-92.
14. Wadler P., Findler R. B. Well-Typed Programs Can't Be Blamed //ESOP. – 2009. – Т. 9. – С. 1-16.
15. Siek J. G., Wadler P. Threesomes, with and without blame //ACM Sigplan Notices. – ACM, 2010. – Т. 45. – №. 1. – С. 365-376.
16. Siek J., Wadler P. The key to blame: Gradual typing meets cryptography. – 2016.
17. Kosikov S. V., Wolfengagen V. E., Ismailova L. Yu. The Presentation of Evolutionary Concepts //First International Early Research Career Enhancement School on Biologically Inspired Cognitive Architectures. – Springer, Cham, 2017. – С. 113-125.
18. Ismailova L. Yu., Kosikov S. V., Wolfengagen V. Applicative Methods of Interpretation of Graphically Oriented Conceptual Information //Procedia Computer Science. – 2016. – Т. 88. – С. 341-346.
19. Исмаилова Л. Ю. Модели представления изменяемых объектов // Сборник научных трудов SWorld. 2014. Т. 6. № 2. С. 8-13.
20. Вольфенгаген В. Э. Конструкции языков программирования. – ООО «ЮрИнфоР-Пресс», 2001.

ВЫЯВЛЕНИЕ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ С ПОЗИЦИИ НАРУШЕНИЯ КИБЕРБЕЗОПАНСОТИ НА ПРИМЕРЕ ЭНРЕГЕТИКИ

Д.А. Гаськова
(Иркутск, Институт систем энергетики им. Л.А. Мелентьева СО РАН)
e-mail: gaskovada@gmailcom
Identify

THE IDENTIFICATION OF CRITICAL FACILITIES FROM THE POSITION OF CYBERSECURITY VIOLATION BY THE EXAMPLE OF ENERGY

D. Gaskova
(Irkutsk, Melentiev Energy Systems Institute of SB RAS)

Abstract. The article describes methods for identification of critical facilities, being a significant trend in researching critical infrastructures, particularly in the energy sector. The proposed methods are focused on the investigation of the energy object state in relation to the violation of cybersecurity of its information infrastructure. The cyber threats are believed to be important contemporary threats to energy security in Russia. The proposed methods formed the basis of development information-analytical system used for monitoring of cybersecurity violations in energy sector.
Key words: cybersecurity, cyber threats, semantic models, critical infrastructures, energy facilities

Введение. В период активной информатизации всех сфер жизни общества, была выявлена, в первую очередь на западе [1], необходимость обеспечения защищенности информа-

ции, информационных систем и баз данных, сетей передачи данных и аппаратно-программных комплексов организации. К нарушению безопасности и причинению ущерба компании могут привести как злоумышленники путем проведения атак на IT-ресурсы организации, так и случайные или умышленные действия сотрудников, проявивших халатность в работе [2]. Состояние такой защищенности принято называть кибербезопасностью, которая находится на стыке таких направлений как информационная безопасность, безопасность приложений, сетевая безопасность, безопасность Интернет, защита ключевых информационных систем объектов критической инфраструктуры, но не является синонимом ни одного из них. Последнее из перечисленных направлений включено в приоритетные во многих странах мира исследования критической инфраструктуры, выход из строя либо уничтожение которой может привести к губительным последствиям в области обороны, экономики, здравоохранения и безопасности нации [1]. Энергетику относят к одной из важнейших критических инфраструктур, а энергетическая безопасность является немаловажной составляющей национальной безопасности страны [3]. Ключевая особенность нарушения кибербезопасности заключается в возможности нарушения нормального функционирования, вплоть до вывода из строя, как нематериальных, так и физических объектов путем влияния на них из информационной среды.

В данной статье предлагается выявлять критически важные объекты (КВО) в энергетике на основе оценки защищенности от киберугроз информационно-технологической (ИТ) системы энергетического объекта (ЭО), с учетом территориального критерия расположения ЭО, возможного влияния объектов близлежащий критических инфраструктур (на основе исследований энергетической безопасности), а также вероятности наступления каскадных аварий.

Методы выявления критически важных объектов. Исследование критических инфраструктур является обширной многокритериальной задачей, включающей выявление критически важных объектов каждой инфраструктуры отдельно и их взаимного влияния. Выявление КВО предлагается осуществлять в три этапа, включающие следующие методы:

1. методы выявления уязвимостей и угроз ИТ системы ЭО;
2. методы анализ угроз с использованием семантического моделирования;
3. методы анализа рисков нарушения кибербезопасности критической информационной инфраструктуры.

Первый этап заключается в выявлении уязвимостей анализируемых ЭО. Осуществляется выбор анализируемых ЭО, производится их описание и установление взаимосвязей, выявления типовых уязвимостей ИТ системы каждого ЭО на заданной территории. Объекты при этом подразделяются на объекты выработки, транспортировки и потребления энергии. Для поддержки этапа разрабатывается научный прототип продукционной экспертной системы «Cyber». Применение методов геовизуализации позволит инженеру-исследователю в области энергетики наглядно определять местоположение объектов относительно друг друга, а также, при большом количестве объектов, переключаться на режим отображения основных характеристик выявленных уязвимостей и угроз каждого ЭО.

На втором этапе осуществляется построение сценариев реализации угроз на анализируемых ЭО на основе сценарного похода. Строится вероятностная модель наступления угроз энергетической безопасности при условии реализации киберугроз, выявленных на предыдущем этапе, и последствий от них. Вероятностная модель строится с использованием Байесовских сетей доверия.

Третий этап включает оценку рисков и последствий каждого сценария с применением риск-ориентированного подхода. Данный подход учитывает ущерб от повреждения или уничтожения объекта с использованием качественных и количественных параметров, а также вероятность повреждения или уничтожения компонентов объекта, с учетом масштабов ущерба и возможности наступления каскадных аварий. Риски определяются тройкой: угрозы, уязвимости, ущербы [4]. Оценка рисков производится на основе полученных вероятно-

стей угроз, разработанной классификации рисков, а также предполагаемых последствий с точки зрения критериев оценки и экономической эффективности. Для поддержки этапа реализован прототип «RiskMap», позволяющий строить тепловую карту рисков и лепестковую диаграмму в зависимости от классификации типов рисков.

Общий алгоритм выявления КВО представлен на рисунке 1.

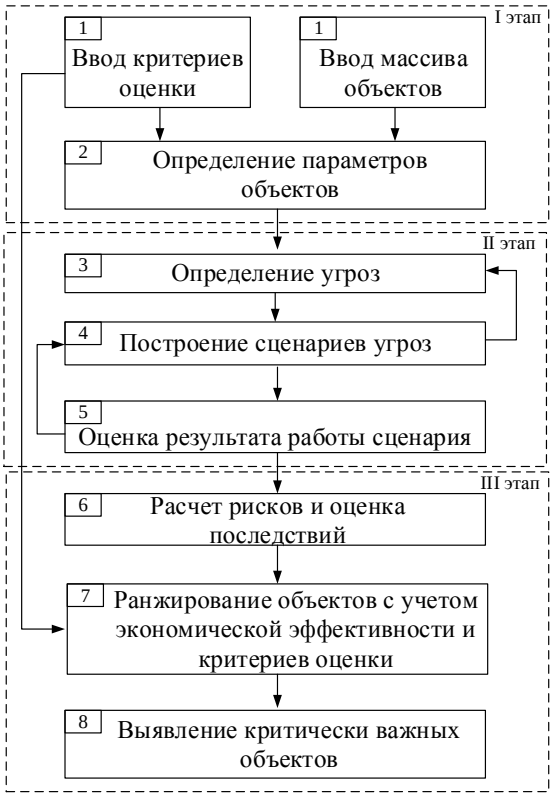

Рис. 1. Этапы выявления КВО

На первом шаге определяются критерии, на основе которых будет решаться принадлежность объекта энергетики к КВО. Критерии могут быть, например, связанные как с масштабами потребления топлива, так и качеством жизни населения в данном регионе [5]. Определятся полный набор объектов для решения задачи выявления КВО по стране, в регионе, муниципалитете или иной территориальной единице.

На втором шаге для каждого объекта: определяется тип объекта; формируется его паспорт безопасности; выявляются уязвимости кибербезопасности на организационно-правовом, техническом и оперативном уровнях.

На третьем шаге на основе информации об объекте и его уязвимостях осуществляется установление взаимосвязей между уязвимостями и возможными киберугрозами, с учетом уже существующих превентивных мер нарушения безопасности.

Далее осуществляется построение сценариев реализации угроз для каждого объекта, либо для моделирования некоторой критической ситуации, включающей несколько объектов, например, при каскадных авариях.

На пятом шаге осуществляется оценка результатов сценариев. Экспертно выбираются наиболее вероятные, либо отвечающие критериям оценки, также определяются часто-задействованные объекты при множественных сценариях и наиболее уязвимые активы в сценариях для одного объекта.

На шестом шаге осуществляется расчет рисков для каждого объекта и визуализация их на карте риска для осуществления дальнейшего экспертного анализа.

На седьмом шаге на основе рассчитанных рисков с учетом экономической эффективности и принятых критериев оценки осуществляется ранжирование энергетических объектов. Заключительный шаг состоит в определении КВО и принятии дальнейших решений по обеспечению контрмер от критических ситуаций.

Заключение. В связи с отсутствием утвержденной методики выявления КВО в критических инфраструктурах и тенденцией внедрения современных информационно-коммуникационных технологий в энергетике предлагается применять описанные методы, включающие моделирование и анализ критических ситуаций, возникающих при реализации киберугроз. На основе данных методов и методики анализа угроз и оценки рисков [6] разрабатывается интеллектуальная система [7], поддерживающая основные этапы выявления КВО.

Работа выполнена в рамках научного проекта III.17.2.1 программы фундаментальных исследований СО РАН, рег. № АААА-А17-117030310444-2, и при частичной финансовой поддержке грантов РФФИ №17-07-01341 и № 18-07-00714.

ЛИТЕРАТУРА

1. Кондратьев А. Современные тенденции в исследовании критической инфраструктуры в зарубежных странах // Зарубежное военное обозрение. 2012. № 1. С. 19–30.
2. Массель А.Г. Кибератаки как угроза энергетической безопасности России / Труды Международной конференции «Кибербезопасность-2013». – Украина, Киев, Институт специальной связи и защиты информации НТУ Украины «КПИ», 2013. – С. 49-56.
3. Массель Л.В., Воропай Н.И., Сендеров С.М., Массел А.Г. Киберопасность как одна из стратегических угроз энергетической безопасности // Вопросы кибербезопасности. №4 (17). 2016. – С 2-10.
4. Массель Л.В., Массель А.Г., Гаськова Д.А. Кибербезопасность в критических инфраструктурах (на примере энергетики) // Сборник трудов Седьмой Всероссийской научно-технической конференции «Безопасные информационные технологии» (БИТ-2016) //Под редакцией В.А. Матвеева. 2016. С. 197-199.
5. Массель Л. В. Конвергенция исследований критических инфраструктур, качества жизни и безопасности / Информационные технологии и системы: Труды Шестой Международной научной конференции ИТиС-2017. Челябинск: ЧелГУ. Науч. электрон. издание. ISBN 978-5-7271-1417-9. – С. 170-175.
6. Массель А.Г. Методика анализа угроз и оценки риска нарушения информационно-технологической безопасности энергетических комплексов // Информационные и математические технологии в науке и управлении / Ответственный редактор Л.В. Массель. 2015. С. 186-195.
7. Massel A.G., Gaskova D.A. Application of risk-based approach to identify critical facilities in the energy sector with regard to cyber threats // Proceedings of the 19th International Workshop on Computer Science and Information Technologies. Germany, Baden-Baden. Publisher Ufa: USATU. Vol. 1. 2017. – Pp. 159-163. ISBN 978-5-1030-8, ISBN 978-4-4221-1031-5 (v. 1)