УДК 004.8

ПОДХОД К ОЦЕНКЕ РИСКОВОГО ПОТЕНЦИАЛА ЗНАЧИМЫХ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

А.О. Калашников
Институт проблем управления им. В.А. Трапезникова РАН
Россия, 117997, Москва, Профсоюзная ул., 65
E-mail: aokalash@ipu.ru

Е.А. Сакрутина
Институт проблем управления им. В.А. Трапезникова РАН
Россия, 117997, Москва, Профсоюзная ул., 65
E-mail: consoft@ipu.ru

Ключевые слова: критическая информационная инфраструктура, значимый объект критической информационной инфраструктуры, оценка рискового потенциала.

Аннотация: В работе рассматривается подход к оценке рискового потенциала значимых объектов критической информационной инфраструктуры основанный на прогнозировании выхода технологического процесса на аварийные режимы на значимых объектах критической информационной инфраструктуры.

1. Введение

Приоритетной целью государственной политики на сегодняшний день является обеспечение информационной безопасности объектов критической информационной инфраструктуры Российской Федерации. В соответствии с действующим Федеральным законом от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [1] (далее – ФЗ от 26.07.2017 № 187-ФЗ), введены такие понятия как: критическая информационная инфраструктура (далее – КИИ), объекты КИИ, субъекты КИИ, значимый объект КИИ (далее – ЗОКИИ), безопасность КИИ. К ЗОКИИ относятся крупные гидротехнические сооружения, объекты атомной энергетики, вредные химические производства, нефтеперерабатывающие заводы, газопроводы, транспортные системы и т.п. Сбой в работе любого из объектов ЗОКИИ может отразится на здоровье, безопасности и благосостоянии граждан [2].

В соответствии с ФЗ от 26.07.2017 № 187-ФЗ будем полагать, что КИИ РФ состоит из объектов двух основных типов: ЗОКИИ и сетей электросвязи, используемые для организации взаимодействия таких объектов. Состояние ЗОКИИ может быть описано текущим уровнем информационной безопасности (далее – УИБ) и связанным с ним рисковым потенциалом (далее – РП). УИБ ЗОКИИ определяется текущим уровнем информационных угроз (далее – УИУ) и текущим уровнем защищенности (далее – УЗ) ЗОКИИ. В свою очередь, РП представляет собой прогнозную оценку последствий нарушения функционирования ЗОКИИ, при реализации компьютерных атак на ЗОКИИ и

возникновении в результате этого компьютерных инцидентов. Оценка РП ЗОКИИ может быть представлена в многокритериальной (векторной) форме, учитывающей РП ЗОКИИ по отдельным направлениям, определенным ФЗ от 26.07.2017 № 187-ФЗ. На основании векторной оценки РП может быть построена интегральная оценка РП ЗОКИИ. При оценке РП ЗОКИИ следует отметить следующие особенности: во-первых, интегральный РП ЗОКИИ складывается из совокупности локальных РП ЗОКИИ, во-вторых, РП ЗОКИИ можно измерить лишь качественно (высокий, средний, низкий), в-третьих, оценка РП ЗОКИИ носит субъективный характер [3].

2. Уровни модели ЗОКИИ РФ

Воздействие компьютерных атак на информационно-технологическую инфраструктуру (далее – ИТИ) ЗОКИИ, приводящее к выходу ее технологических параметров за установленные нормативные пределы, может повлечь за собой реализацию нештатных ситуаций с тяжелыми и даже катастрофическими последствиями. Для успешной реализации мероприятий защиты ЗОКИИ необходимо решение ряда задач, из которых система мониторинга угроз безопасности является основной.

В последние годы, системные причины многих инцидентов на ЗОКИИ привели к существенному повышению интереса к процедурам идентификации и управления рисками [4], а также разработке и развитию проактивных моделей. Проактивные модели дают оценку РП выявленных факторов прежде чем произойдет инцидент и окажет влияние на функционирование ЗОКИИ.

Предположим, что модель ЗОКИИ состоит из трех взаимосвязанных уровней (см. рис. 1). Подробнее см., например, [5-7].

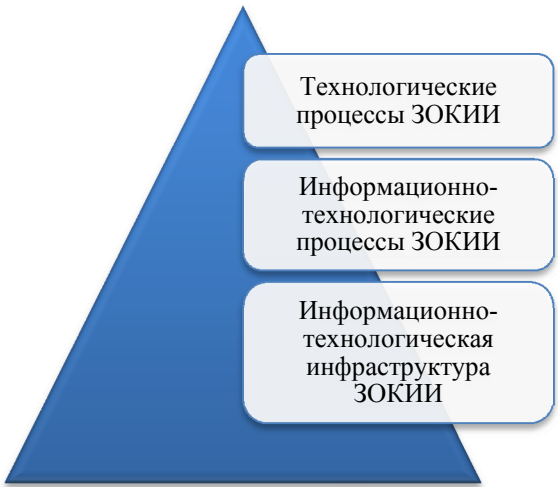

Рис. 1. Уровни модели значимого объекта критической информационной инфраструктуры.

Верхний уровень – уровень «технологических» (бизнес) процессов (далее – ТП) ЗОКИИ. Состояние ТП может быть описано текущим вектором значений параметров $X^{\text{ТП}}(t) = \{x_1^{\text{ТП}}(t), \dots, x_N^{\text{ТП}}(t)\}$. Состояние ТП ЗОКИИ, в свою очередь, определяет текущий РП ЗОКИИ $R(t) = \{r_1(t), \dots, r_p(t)\}$. Если значения вектора параметров не выходят за границы эксплуатационных пределов и установленных условий функционирования ЗОКИИ, то такое состояние ТП ЗОКИИ может считаться нормальным, а РП ЗОКИИ

соответствует допустимому уровню. В противном случае, состояние ТП ЗОКИИ может считаться аварийным, а РП ЗОКИИ будет превышать допустимый уровень.

Средний уровень – уровень информационно-технологических процессов (далее – ИТП). Состояние ИТП также может быть описано вектором параметров $X^{\text{ИТП}}(t) = \{x_1^{\text{ИТП}}(t), \dots, x_M^{\text{ИТП}}(t)\}$ (в общем случае отличным от вектора параметров ТП). Для обеспечения нахождение ТП в нормальном состоянии, значения вектора параметров ИТП также должны находиться в определенных диапазонах, которые будем считать диапазонами нормальных значений параметров ИТП.

Нижний уровень – уровень информационно-технологической инфраструктуры (далее – ИТИ) ЗОКИИ, обеспечивающий нормальное функционирование ИТП ЗОКИИ. Будем считать, что состояние ИТИ может быть описано вектором параметров $X^{\text{ИТИ}}(t) = \{x_1^{\text{ИТИ}}(t), \dots, x_S^{\text{ИТИ}}(t)\}$ (в общем случае отличным от вектора параметров ТП и ИТП). Тогда, чтобы обеспечить нахождение ИТП в нормальном состоянии, значения вектора параметров ИТИ должны находиться в некоторых определенных диапазонах, которые будем считать диапазонами нормальных значений параметров ИТИ. Если значения вектора параметров ИТИ находятся в пределах указанных выше диапазонов нормальных значений, то такое состояние ИТИ ЗОКИИ может считаться нормальным. Если значения вектора параметров ИТИ выходят за диапазоны нормальных значений, то такое состояние ИТИ ЗОКИИ может считаться аварийным. Следовательно, параметры вектора состояния ИТИ ЗОКИИ будем называть *критическими переменными состояния*.

Таким образом, можно считать, что существует определенная «функциональная» зависимость между состоянием ИТИ ЗОКИИ и РП ЗОКИИ. При построении модели ЗОКИИ представляется достаточным ограничиться построением параметрической модели ИТИ ЗОКИИ и некоторой регрессионной моделью, описывающей зависимость вектора РП от параметров ИТИ.

Теоретические аспекты критических переменных состояния и их экстремальных значений нашли свое применение при описании ИТИ ЗОКИИ [7]. Примерами могут служить работы [5, 6, 8, 9].

3. Модели оценки рискового потенциала ИТИ ЗОКИИ

Предположим, что данные об оценках РП и критических переменных состояния ИТИ ЗОКИИ содержатся в некоторой пополняемой базе знаний (далее – БЗ), в которую заносятся данные о функционировании ИТИ ЗОКИИ. Пусть $x_1(t), \dots, x_S(t)$ – параметры состояния ИТИ ЗОКИИ (включая критические переменные состояния), $X(t)$ – состояние ИТИ ЗОКИИ характеризующееся вектором параметров состояния ИТИ ЗОКИИ в момент времени t, $R(t)$ – РП состояния $X(t)$ ИТИ ЗОКИИ в момент времени t. Процесс обработки исторических данных в базе знаний сводится к ассоциативному поиску состояний ИТИ ЗОКИИ близких к текущему. Критерий близости между состояниями может быть представлен в виде расстояния в n-мерном пространстве.

В работах [10-15] предложен подход к формированию поддержки принятия решения об управлении, основанный на динамическом моделировании процедуры ассоциативного поиска. Прогнозирование РП ИТИ ЗОКИИ заключается в качественной оценке локальных РП по прогнозу на основе ассоциативного поиска критических переменных состояния в части выхода за диапазоны нормальных значений. Ассоциативный поиск заключается в построении в каждый момент времени виртуальных прогнозирующих моделей. Пусть линейная динамическая модель ИТИ ЗОКИИ имеет следующий вид:

(1) $$K(t) = \sum_{i=1}^{m} a_i K(t-i) + \sum_{j=1}^{r_s} \sum_{s=1}^{S} b_{j,s} x_s(t-j),$$

где $K(t)$ – прогноз критической переменной состояния в момент времени t, x_s – параметр состояния ИТИ ЗОКИИ, m – глубина памяти по критическому параметру безопасности на уровне ИТИ ЗОКИИ, S – размерность вектора параметров состояния ИТИ ЗОКИИ, a_i и $b_{j,s}$ – настраиваемые коэффициенты. Причем, модель (1) не является классической регрессионной моделью, так как при построении модели из БЗ ИТИ ЗОКИИ выбираются в каждый момент времени $x_s(t-j)$ близкие к текущему вектору параметров состояния в смысле определенного критерия., а r_s является глубиной памяти вектора параметров состояния.

Вывод условий устойчивости прогнозирующей модели на основе вейвлет-разложения приведен в [16]. Не выполнение условий устойчивости прогнозирующей модели указывает на вероятность сохранения тенденции к увеличению или уменьшению оценки безопасности на следующем такте времени. Таким образом, можно определить опасные события, которые в будущем могут нарушить безопасность КИИ, что является актуальным для ЗОКИИ. Например, для атомных электростанций такой подход позволит в рамках информационной системы поддержки операторов [17] выделить сверхнормативные материальные и энергетические балансы в работе АЭС и места их возникновения, что в свою очередь позволяет диагностировать аномалии [18].

4. Проблема достаточного количества векторов состояния

Построение виртуальной модели, соответствующей некоторому моменту времени t, осуществляется посредством выборки из БЗ ИТИ ЗОКИИ близких состояний ИТИ ЗОКИИ к текущему. Далее на основе классического (не рекуррентного) МНК определяется значения критических переменных состояния ИТИ ЗОКИИ в следующий момент времени. На этапе отбора из БЗ ИТИ ЗОКИИ близких состояний ИТИ ЗОКИИ к текущему, имеется несколько проблем:

- недостаточное количество векторов состояния ИТИ ЗОКИИ для применения МНК,
- снижение точности прогноза за счет переизбытка векторов состояния ИТИ ЗОКИИ.

Если векторов состояния ИТИ ЗОКИИ недостаточно, то можно ослабить критерий отбора векторов из БЗ ИТИ ЗОКИИ. При переизбытке векторов состояния ИТИ ЗОКИИ можно усилить критерий отбора, но такой подход может не дать видимых результатов.

Критерием достаточности векторов состояния для построения модели на основе ассоциативного поиска является минимум ошибки прогноза. Обратимся к качественным показателям прогноза – средняя абсолютная ошибка (mean absolute error – MAE) и среднеквадратическая ошибка (mean squared error – MSE) [19]. Показатель прогноза MAE применяется для оценки точности прогноза и вычисляется по формуле (2):

(2) $$MAE = \frac{1}{N} \sum_{i=1}^{N} |y_i(t) - \tilde{y}_i(t)|,$$

где $y_i(t)$ – фактическое значение, $\tilde{y}_i(t)$ – прогнозируемое значение, N – количество рассматриваемых тактов. Показатель прогноза MSE чувствителен к появлению больших ошибок при прогнозировании и вычисляется по формуле (3):

(3) $$MSE = \frac{1}{N} \sum_{i=1}^{N} \left(y_i(t) - \tilde{y}_i(t)\right)^2.$$

Таким образом, для отбора достаточного количества векторов состояния из БЗ ИТИ ЗОКИИ необходимо провести вычислительный эксперимент на тестовой выборке в зависимости от заданного количества отбираемых векторов состояния. По итогам вычислительного эксперимента необходимо провести сравнение показателей точности прогноза по критериям $MAE \to min$ и $MSE \to min$.

5. Заключение

В работе предложен подход к оценке РП ИТИ ЗОКИИ в части выхода критических переменных состояния за допустимые эксплуатационные пределы. Предложенный подход предназначен для применения в системе мониторинга угроз безопасности ЗОКИИ.

Список литературы

1. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
2. Хочешь мира - готовься к кибервойне! / Акимов Е. // !Безопасность деловой информации. 2013. №2. С. 9-16. URL: http://bis-expert.ru/sites/default/files/miscellaneous/bdi/BDI_2013_2.pdf (дата обращения: 01.12.2017).
3. Калашников А.О. Управление информационными рисками организационных систем: механизмы комплексного оценивания // Информация и безопасность. 2016. Т. 19, № 3. С. 315-322.
4. Sakrutina E. Some Functions of the “Safety management system” in the Transportation Area Safety Assurance // Proceedings of the IEEE International Siberian Conference on Control and Communications (SIBCON-2017, Astana). 2017. P.1-5.
5. Ермилов Е.В., Остапенко Г.А., Калашников А.О. Функции ущерба и риска при описании отказов информационных систем критически важных объектов // Информация и безопасность. 2013. Т. 16. № 2. С. 247-248.
6. Калашников А.О., Ермилов Е.В., Чопоров О.Н., Разинкин К.А., Баранников Н.И. Атаки на информационно-технологическую инфраструктуру критически важных объектов: оценка и регулирование рисков. Воронеж: Научная книга, 2013. 160 с.
7. Калашников А.О., Ермилов Е.В., Бурса М.В., Бабаджанов Р.К., Кургузкин В.А. К вопросу о дискретизации критичных переменных состояния информационно-технологической инфраструктуры критически важного объекта // Информация и безопасность. 2014. Т. 17, № 4. С. 536-547.
8. Ермилов Е.В., Калашников А.О., Корнеева Н.Н., Пастернак Ю.Г. Информационно-технологическая инфраструктура критически важного объекта: специфика регулирования рисков и защита: тезисы // 4 Воронежский форум инфокоммуникационных и цифровых технологий. «Перспективные исследования и разработки в области информационных технологий и связи». Воронеж, 2014. С. 59.
9. Ермилов Е.В., Калашников А.О. Методика управления информационными рисками атакуемых автоматизированных систем управления критически важных объектов // Информация и безопасность. 2013. Т. 16, № 3. С. 379-382.
10. Сакрутина Е.А., Бахтадзе Н.Н. Идентификация систем на основе вейвлет-анализа // Труды XII Всероссийского совещания по проблемам управления (ВСПУ-2014, Москва). 2014. С. 2868-2889.
11. Шоберг А.Г. Анализ одномерного сигнала на основе нечетного и четного базисов вейвлетов с компактными носителями // Интеллектуальные системы. 2012. Т. 33., № 3. С. 150-157.
12. Яковлев А. Н. Введение в вейвлет-преобразования: учебное пособие. НГТУ, 2003. 104 с.
13. Bakhtadze N., Lototsky V.A., Maximov E., Pavlov B.V. Associative Search Models in Industrial systems // IFAC Proceedings Volumes. 2007. Vol. 40, No. 3. P. 105-108.
14. Bakhtadze N.N., Yadykin I.B., Lototsky V.A., Maximov E.M., Sakrutina E.A. Multi-agent Approach to Design of Multimodal Intelligent Immune System for Smart Grid // IFAC Proceedings Volumes. 2013. Vol. 46, No. 9, P. 1164-1169.
15. Váňa Z., Preisig H.A. System identification in frequency domain using wavelets: Conceptual remarks // Systems & Control Letters. 2012. Vol. 61, No. 10. P. 1041-1051.

16. Bakhtadze N.N., Sakrutina E.A. Applying the Multi-Scale Wavelet-Transform to the Identification of Non-linear Time-varying Plants // IFAC-PapersOnLine. Vol. 496, No 12, 2016. P. 1927-1932.
17. Jharko E.Ph. Towards the problem of creating information operator support systems for nuclear power plants // Proceedings of the 2th IEEE International Conference on Control in Technical Systems (CTS), 2017. P. 356-359.
18. Jharko E.Ph. Towards the implementation of the task of calculating technical and economical indexes for nuclear power plants // Proceedings of 2017 International Siberian Conference on Control and Communications (SIBCON), 2016. P. 1-7.
19. Kassam S. The mean-absolute-error criterion for quantization // Acoustics, Speech, and Signal Processing, 1977 IEEE International Conference on Acoustics (ICASSP'77), Vol. 2. 1977. P. 632-635.