УДК 004.8
ББК 32.97

МОДЕЛЬ ПРОГНОЗИРОВАНИЯ РИСКОВОГО ПОТЕНЦИАЛА ЗНАЧИМЫХ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Калашников А. О.[1], Сакрутина Е. А.[2]
(*Институт проблем управления им. В.А. Трапезникова РАН, Москва*)

В работе рассматривается модель прогнозирования рискового потенциала для системы мониторинга угроз безопасности выхода технологического процесса на аварийные режимы на значимых объектах критической информационной инфраструктуры.

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

1. Введение

Приоритетной целью государственной политики на сегодняшний день является обеспечения информационной безопасности объектов критической информационной инфраструктуры Российской Федерации. В соответствии с недавно принятым Федеральным законом от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [9] (далее – ФЗ от 26.07.2017 № 187-ФЗ), который вступает в силу с 01.01.2018, введены такие понятия как: крити-

[1] *Калашников Андрей Олегович*, *доктор технических наук*, *ведущий научный сотрудник* (*Москва, ул. Профсоюзная, д.* 65*, тел.* (*495*) *334-91-11, aokalash@ipu.ru*).
[2] *Сакрутина Екатерина Алексеевна*, *научный сотрудник* (*Москва, ул. Профсоюзная, д.* 65*, тел.* (*495*) *334-91-09, consoft@ipu.ru*).

ческая информационная инфраструктура (далее – КИИ), объекты КИИ, субъекты КИИ, значимый объект КИИ (далее – ЗОКИИ), безопасность КИИ.

Под КИИ понимаются – «объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов». В свою очередь, *объектами* КИИ являются – «информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры», а *субъектами* – «государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей.

Среди всех объектов КИИ выделяют подмножество так называемых ЗОКИИ, где под *значимым объектом* понимается – «объект критической информационной инфраструктуры, которому присвоена одна из категорий значимости и который включен в реестр значимых объектов критической информационной инфраструктуры». К ЗОКИИ могут относится крупные гидротехнические сооружения, объекты атомной энергетики, вредные химические производства, транспортные узлы, аэропорты и т.п.

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 информаци-

онных 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: социальный риск; политический риск; экономический риск; экологический риск; риск для обеспечения обороны, безопасности и правопорядка. На основании векторной оценки РП может быть построена интегральная оценка РП ЗОКИИ (подробнее см., например, [6]).

2. Уровни модели ЗОКИИ

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. Основными целями системы мониторинга угроз безопасности являются снижение РП до минимального и минимизация возникающего ущерба.

В последние годы, системные причины многих инцидентов на ЗОКИИ привели к существенному повышению интереса к процедурам идентификации и управления рисками [16], а также разработке и развитию проактивных моделей. Основной акцент в проактивных моделях делается на профилактике угроз возникновения инцидента (опасного события) путем выявления опасных факторов и принятии мер по уменьшению риска. 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, [3-5].

Верхний уровень – уровень «технологических» (бизнес) процессов (далее – ТП) ЗОКИИ. Каждый ТП может быть описан набором (вектором) параметров $x_1^{\text{ТП}}(t), \dots, x_N^{\text{ТП}}(t)$, исходя из установленных эксплуатационных пределов и условий функционирования ТП ЗОКИИ. Тогда состояние ТП может быть описано текущим вектором значений параметров $(X^{\text{ТП}}(\tilde{t}) = \{x_1^{\text{ТП}}(\tilde{t}), \dots, x_N^{\text{ТП}}(\tilde{t})\})$. Состояние ТП ЗОКИИ, в свою очередь, определяет текущий РП ЗОКИИ $R(t)$. Если значения вектора параметров не выходят за границы эксплуатационных пределов и установленных условий функционирования ЗОКИИ, то такое состояние ТП ЗОКИИ может считаться нормальным. В этом случае будем считать, что РП ЗОКИИ соответствует допустимому уровню. Если значения вектора параметров выходят за границы значений, вытекающих из установленных эксплуатационных пределов и условий функционирования ЗОКИИ, то такое состояние ТП ЗОКИИ может считаться аварийным. В этом случае РП ЗОКИИ будет превышать допустимый уровень.

Рис. 1. Уровни модели ЗОКИИ

Средний уровень – уровень информационно-технологических процессов (далее – ИТП), которые обеспечивают нормальное функционирование ТП. Будем считать, что каждое состояние ИТП $X^{\text{ИТП}}(t)$ также может быть описано вектором параметров $x_1^{\text{ИТП}}(t), \dots, x_M^{\text{ИТП}}(t)$ (в общем случае отличным от вектора параметров ТП). Тогда, для того, чтобы обеспечить нахождение ТП в нормальном состоянии, значения вектора параметров ИТП также должны находиться в определенных диапазонах, которые будем считать диапазонами нормальных значений параметров ИТП. Если значения вектора параметров ИТП находятся в пределах указанных выше диапазонов нормальных значений, то такое состояние ИТП ЗОКИИ может считаться нормальным. Если значения вектора параметров ИТП выходят за диапазоны нормальных значений, то такое состояние ИТП ЗОКИИ может считаться аварийным. Очевидно, что в этом случае, если ИТП ЗОКИИ находится в аварийном состоянии, то и ТП ЗОКИИ находится в аварийном состоянии.

Нижний уровень – уровень информационно-технологической инфраструктуры (далее – ИТИ) ЗОКИИ, обеспечивающий функционирование ИТП ЗОКИИ. Будем считать, что состояние ИТИ $X^{\text{ИТИ}}(t)$ также может быть описано вектором параметров $x_1^{\text{ИТИ}}(t), \dots, x_S^{\text{ИТИ}}(t)$ (в общем случае отличным от вектора параметров ТП и ИТП). Тогда, для того, чтобы обеспечить нахождение ИТП в нормальном состоянии, значения вектора параметров ИТИ также 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. Очевидно, что в этом случае, если ИТИ ЗОКИИ находится в аварийном состоянии, то ИТП ЗОКИИ, следовательно, и ТП ЗОКИИ находятся в аварийном состоянии. С учетом сказанного выше, параметры вектора параметров, описывающего состояние ИТИ ЗОКИИ будем называть *критическими переменными состояния*.

Таким образом, можно считать, что существует определенная «функциональная» зависимость между состоянием ИТИ ЗОКИИ, описываемым вектором параметров ИТИ, и РП ЗОКИИ, описываемым вектором РП $R(t)$. Отклонение состояния ИТИ ЗОКИИ от нормального приводит к соответствующему отклонению РП ЗОКИИ от допустимого уровня. Параметры указанной выше зависимости могут быть определены экспертно-аналитическими методами в сочетании с методами анализа данных и стохастического имитационного моделирования. Таким образом, учитывая вышесказанное, 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 [5]. Примерами могут служить работы [1-4]. Базовой методологией оценки безопасности ЗОКИИ является сравнение экстремальных значений переменных состояния с предельно допустимыми значениями.

На современном этапе развития ЗОКИИ невозможно обойтись без широкого применения автоматизированных систем управления технологическими процессами (АСУ ТП). Одной из целей атак на АСУ ТП является вывод технологического процесса на критические (аварийные) режимы, когда значения критических переменных состояния выходят за эксплуатационные пределы и приводят к значительным ущербам и авариям. Одним из примеров такой атаки может служить применение компьютерного червя Stuxnet, поразившего в 2010 г. ядерные объекты Ирана. Stuxnet был ориентирован на выведение из строя турбогенератора путем скачкообразного изменения частоты вращения свыше допустимых эксплуатационных пределов. Из-за «человеческого фактора» Stuxnet поразил ряд компьютеров на АЭС «Бушер», но это не привело к аварии на станции, так как не были заражены компьютеры турбинного отделения.

Избежать выхода ТП на критические режимы, можно используя прогнозирующие модели в системе мониторинга угроз безопасности. В настоящее время существуют методы прогно-

зирования временных рядов на основе вейвлет-анализа, как например [7, 10], но существенным недостатком такого подхода является фактор не учета связности параметров объекта.

Исходные данные для построения моделей могут быть получены в процессе проведения категорирования объектов КИИ и оценки защищенности ЗОКИИ. Далее параметры модели ЗОКИИ могут изменяться при появлении дополнительной информации об изменении структуры ИТИ, появлении новых информационных угроз, воздействий компьютерных атак, результатов расследования компьютерных инцидентов и т.д.

3. Модель 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 $\tilde{t}$ ($X(t) = \{x_1(\tilde{t}), \dots, x_S(\tilde{t})\}$), $R(\tilde{t})$ – РП состояния $X(\tilde{t})$ ИТИ ЗОКИИ в момент времени $\tilde{t}$. Процесс обработки исторических данных в базе знаний сводится к ассоциативному поиску состояний ИТИ ЗОКИИ близких к текущему в базе знаний (см. рис. 2). Критерий близости между состояниями может быть представлен в виде логической функции – предиката, расстояния в n-мерном пространстве.

Процесс ассоциативного поиска может осуществляться либо как процесс восстановления состояния по частично заданным параметрам, либо как процесс поиска связанных ассоциативно с данным состоянием других состояний, привязанных к другим моментам времени. Вместо восстановления состояния ИТИ ЗОКИИ по частично заданным параметрам может осуществляться восстановление фрагмента состояния в условиях неполной информации.

В работах [8, 11-13, 14, 17] предложен подход к формированию поддержки принятия решения об управлении, основанный на динамическом моделировании процедуры ассоциативно-

го поиска. Метод прогнозирования РП ИТИ ЗОКИИ на основе ассоциативного поиска, состоит в построении виртуальных прогнозирующих моделей. Метод предполагает построение новой прогнозирующей модели РП в каждый момент времени t, с использованием исторических данных («ассоциаций»), сформированных на этапе обучения и адаптивно корректируемых в соответствии с определенными критериями.

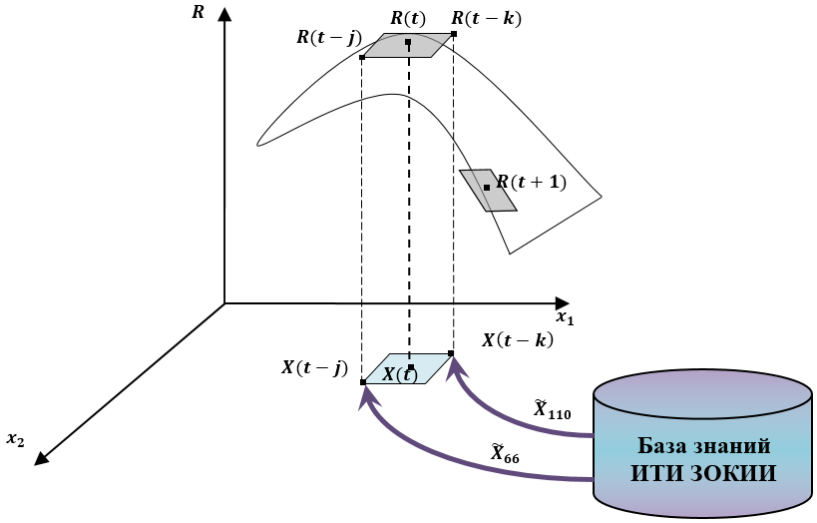

Рис. 2. Ассоциативный поиск в БЗ ИТИ ЗОКИИ.

Пусть линейная динамическая модель РП ИТИ ЗОКИИ имеет следующий вид:

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

где $R(t)$ – прогноз оценки РП ИТИ ЗОКИИ в момент времени t, x_s – параметр состояния ИТИ ЗОКИИ, m – глубина памяти по РП ИТИ ЗОКИИ, S – размерность вектора параметров состояния ИТИ ЗОКИИ, a_i и $b_{j,s}$ – настраиваемые коэффициенты. Причем, при построении модели (1) из БЗ ИТИ ЗОКИИ $x_s(t-j)$ выбираются в каждый момент времени не в хронологическом поряд-

ке, а r_s является количеством векторов параметров состояния выбранных по критерию минимума расстояния из БЗ ИТИ ЗОКИИ.

Модель (1) не является классической регрессионной моделью, так как при построении модели из БЗ ИТИ ЗОКИИ выбираются векторы параметров состояния не в хронологической последовательности, а лишь близкие к текущему вектору параметров состояния в смысле определенного критерия.

Для построения виртуальной модели РП ИТИ ЗОКИИ в данный момент времени по текущему состоянию ИТИ ЗОКИИ воспользуемся следующим критерием отбора входных векторов из базы знаний, приведенным ниже. Введем в качестве расстояния (нормы в $\Re^S$) между точками S-мерного пространства параметров состояния величину:

$$(2)\quad d_{t,t-j} = \sum_{s=1}^{S} |x_s(t) - x_s(t-j)|, \forall j = \overline{1, t-1},$$

где $x_s(t)$ – компоненты вектора состояний ИТИ ЗОКИИ в момент времени t.

В силу одного из свойств нормы («неравенство треугольника») имеем:

$$(3)\quad d_{t,t-j} \le \sum_{s=1}^{S} |x_s(t)| + \sum_{s=1}^{S} |x_s(t-j)|, \forall j = \overline{1, t-1}.$$

Пусть для текущего вектора состояний ИТИ ЗОКИИ $x_s(t)$:

$$(4)\quad \sum_{s=1}^{S} |x_s(t)| = d_t.$$

Для построения аппроксимирующей гиперповерхности для $X(t)$ отберем из архива входных данных такие векторы $x_s(t-j)$, $j = \overline{1, t-1}$, что для некоторого заданного D_t будет выполнено условие:

$$(5)\quad d_{t,t-j} \le d_t + \sum_{s=1}^{S} |x_s(t-j)| \le D_t, \forall j = \overline{1, t-1},$$

где D_N может быть выбрано, например, из условия:

(6) $D_t \geq 2d_t^{max} = 2\max_j \sum_{s=1}^{S} |x_s(t-j)|.$

Если в выбранной области не наберется достаточного количества параметров состояния для применения МНК, т.е. соответствующая система линейных уравнений окажется неразрешимой, то выбранный критерий отбора точек в пространстве входов можно будет ослабить за счет увеличения порога D_t.

В предположении, что входные воздействия удовлетворяют условиям Гаусса-Маркова, оценки, получаемые по методу наименьших квадратов, являются состоятельными, несмещенными и статистически эффективными.

4. Подход к определению достаточного количества векторов состояния

Алгоритм построения виртуальной модели оценки РП ИТИ ЗОКИИ состоит в построении в каждый момент времени аппроксимирующей гиперповерхности пространства параметров состояния ИТИ ЗОКИИ и соответствующих им оценки РП ИТИ ЗОКИИ. Размерность этой гиперповерхности выбирается эвристически. Для построения виртуальной модели, соответствующей некоторому моменту времени t, из БЗ ИТИ ЗОКИИ отбираются близкие состояния ИТИ ЗОКИИ к текущему. Далее на основе классического (не рекуррентного) метода наименьших квадратов (далее – МНК) определяется значение оценки РП ИТИ ЗОКИИ в следующий момент времени. Стоит отметить, что в каждый следующий момент времени каждая точка глобальной нелинейной поверхности регрессии формируется в результате использования линейных «локальных» моделей.

На этапе отбора из БЗ ИТИ ЗОКИИ близких состояний ИТИ ЗОКИИ к текущему в смысле определенного критерия (описанного в разделе 3), имеется несколько проблем:

- недостаточное количество векторов состояния ИТИ ЗОКИИ для применения МНК,
- уменьшение 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 было бы усилить критерий отбора, но он может не дать видимых результатов, так как близких векторов состояния по критерию может быть также достаточно большое количество.

Критерием достаточности векторов состояния для построения модели на основе ассоциативного поиска является минимум ошибки прогноза. Обратимся к качественным показателям прогноза – mean absolute error (MAE) and mean squared error (MSE) [15]. Показатель прогноза MAE применяется для оценки точности прогноза и вычисляется по формуле (7):

$$(7)\quad MAE = \frac{1}{N}\sum_{i=1}^{N}|y_i(t) - \widetilde{y_i}(t)|,$$

где $y_i(t)$ – фактическое значение, $\widetilde{y_i}(t)$ – прогнозируемое значение, N – количество рассматриваемых тактов. Показатель прогноза MSE чувствителен к появлению больших ошибок при прогнозировании и вычисляется по формуле (8):

$$(8)\quad MSE = \frac{1}{N}\sum_{i=1}^{N}\left(y_i(t) - \widetilde{y_i}(t)\right)^2.$$

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

5. Заключение

В работе предложена модель безопасности, позволяющая дать оценку РП ИТИ ЗОКИИ в части выхода критических параметров состояния за эксплуатационные пределы. Предложенная модель предназначена для применения в системе мониторинга угроз безопасности ЗОКИИ.

Литература

1. ЕРМИЛОВ Е. В. *Информационно-технологическая инфраструктура критически важного объекта: специфика регулирования рисков и защита: тезисы* / Е. В. Ермилов, А. О. Калашников, Н. Н. Корнеева, Ю. Г. Пастернак // 4 Воронежский форум инфокоммуникационных и цифровых технологий. «Перспективные исследования и разработки в области информационных технологий и связи». – Воронеж, 2014. – С. 59.
2. ЕРМИЛОВ Е. В. *Методика управления информационными рисками атакуемых автоматизированных систем управления критически важных объектов* / Е. В. Ермилов, А. О. Калашников // Информация и безопасность. – 2013. – Т. 16. № 3. – С. 379-382.
3. ЕРМИЛОВ Е. В. *Функции ущерба и риска при описании отказов информационных систем критически важных объектов* / Е. В. Ермилов, Г. А. Остапенко, А. О. Калашников // Информация и безопасность. – 2013. – Т. 16. № 2. – С. 247-248.
4. КАЛАШНИКОВ А. О. *Атаки на информационно-технологическую инфраструктуру критически важных объектов: оценка и регулирование рисков* / А. О. Калашников, Е. В. Ермилов, О. Н. Чопоров, К. А. Разинкин, Н. И. Баранников; под ред. чл.-корр. РАН Д. А. Новикова. – Воронеж: Издательство «Научная книга», 2013. – 160 с.
5. КАЛАШНИКОВ А. О. *К вопросу о дискретизации критичных переменных состояния информационно-технологической инфраструктуры критически важного объекта* / А. О. Калашников, Е. В. Ермилов, М. В. Бурса, Р. К. Бабаджанов, В. А. Кургузкин // Информация и безопасность – 2014. – Т. 17. № 4. – С. 536-547.
6. КАЛАШНИКОВ А. О. *Управление информационными рисками организационных систем: механизмы комплексного оценивания* / А. О. Калашников // Информация и безопасность. – 2016. – № 3. –С. 315-322.

7. ОСМИНИН К. П. *Алгоритмы построения статистик для анализа и прогнозирования нестационарных временных рядов* / К. П. Осминин // Информационные технологии и вычислительные системы – 2009. – №1: С. 3-13.
8. САКРУТИНА Е. А. *Идентификация систем на основе вейвлет-анализа* / Е. А. Сакрутина, Н. Н. Бахтадзе // Труды XII Всероссийского совещания по проблемам управления (ВСПУ-2014, Москва) – 2014. М.: ИПУ РАН, С. 2868-2889.
9. *Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»*.
10. ЧЕРНЫХ В. Ю. *Прогнозирование нестационарных временных рядов при несимметричных функциях потерь* / В. Ю. Черных, М. М. Стенина // Машинное обучение и анализ данных – 2015. – Т. 1, №14: С. 1893-1909.
11. ШОБЕРГ А. Г. *Анализ одномерного сигнала на основе нечетного и четного базисов вейвлетов с компактными носителями* / А. Г. Шоберг // Интеллектуальные системы – 2012. Т. 33. №3: С. 150-157.
12. ЯКОВЛЕВ А. Н. *Введение в вейвлет-преобразования: учебное пособие* / А. Н. Яковлев // НГТУ, 2003. – 104 с.
13. BAKHTADZE N. *Associative Search Models in Industrial systems* / N. Bakhtadze, V. A. Lototsky, E. Maximov, B. V. Pavlov // IFAC Proceedings Volumes – 2007. Vol. 40, № 3, P. 105-108.
14. BAKHTADZE N. N. *Multi-agent Approach to Design of Multimodal Intelligent Immune System for Smart Grid* / N. N. Bakhtadze, I. B. Yadykin, V. A. Lototsky, E. M. Maximov, E. A. Sakrutina // IFAC Proceedings Volumes – 2013. Vol. 46, № 9, P. 1164-1169.
15. KASSAM S. *The mean-absolute-error criterion for quantization* / S. Kassam // Acoustics, Speech, and Signal Processing, 1977 IEEE International Conference on Acoustics (ICASSP '77) – 1977. Vol. 2, P. 632-635.
16. SAKRUTINA E. A. *Some Functions of the "Safety management system" in the Transportation Area Safety Assurance* / E. Sakrutina // Proceedings of 2017 International Siberian Conference on Control and Communications (SIBCON) – 2017. P. 1-5.

17. VÁŇA Z. *System identification in frequency domain using wavelets: Conceptual remarks* / Z. Váňa, H. A. Preisig // Systems & Control Letters – 2012. Vol. 61, №. 10. P. 1041-1051.

A MODEL OF PREDICTING RISK POTENTIAL OF SIGNIFICANT PLANTS OF CRITICAL INFORMATION INFRASTRUCTURE

Andrey Kalashnikov, Institute of Control Sciences of RAS, Moscow, Doctor of Science, Leading researcher (Moscow, Profsoyuznaya st., 65, (495) 334-91-11, aokalash@ipu.ru).
Ekaterina Sakrutina, Institute of Control Sciences of RAS, Moscow, Researcher (Moscow, Profsoyuznaya st., 65, (495) 334-91-09, consoft@ipu.ru).

Abstract: *In the paper, a model of predicting risk potential for a system of monitoring safety threats of transferring a technological process to alarm modes on significant plants of critical information infrastructure is considered.*

Keywords: critical information infrastructure, significant plant of critical information infrastructure, risk potential assessment, associative search.

Статья представлена к публикации членом редакционной коллегии ...заполняется редактором…

Поступила в редакцию ...заполняется редактором…
Опубликована ...заполняется редактором…