РАЗВИТИЕ СИСТЕМ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ НА ОСНОВЕ ПРЕЦЕДЕНТОВ В РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СТРУКТУРАХ

Бурый А.С.[1], Усцелемов В.Н.[2]

Ключевые слова: *распределенная информационная система, прецедент, информационная безопасность, риск, поддержка принятия решений, система на основе рассуждений, классификатор, метод, модель, алгоритм, сходство.*

Аннотация

Цель работы: развитие адаптивных механизмов подсистемы информационной безопасности в организационных системах поддержки принятия решений на основе метода построения выводов по прецедентам, а также оценки динамики информационного конфликтного взаимодействия, отличающейся возможностью выработки управляющего воздействия для настройки (перенастройки) механизмов подсистемы информационного обмена.

Методы: комплексное использование системного и сравнительного анализа, методов обеспечения информационной безопасности, метода построения рассуждений на основе прецедентов, концептуально-логического обоснования структур построения распределенных информационных систем.

Результаты: обоснован концептуально-методический подход к построению гибридных процедур формирования баз прецедентов на основе метода рассуждений, сочетания метрических методов классификации инцидентов информационной безопасности и алгоритмов экспертного оценивания объектов классификации в задачах мониторинга информационных ресурсов интегрированных информационных структур заданной предметной области; разработана формально-логическая модель настройки подсистемы информационной безопасности на основе рассуждений по прецедентам с использованием модифицированного метода k-ближайших соседей; обоснована рациональная структура базы прецедентов и эффективный алгоритм поиска прецедентов.

EDN: XTRUMB

Введение

Одной из характерных особенностей информации является множество различных форм ее существования, проявления и представления [11]. С одной стороны, это позволяет использовать и развивать организационные подходы к построению *распределенных информационных систем*, совершенствовать их информационное, модельно-алгоритмическое, техническое и др. обеспечение, формировать *требования* к информационным ресурсам и технологиям. С другой стороны, появляется дополнительная опасность при обращении с информацией в контурах управления и принятия решений, связанная с необходимостью обеспечить ее *сохранность* в условиях различного рода воздействий (случайных и преднамеренных).

Процесс построения эффективной *подсистемы защиты* информационной системы часто представляет собой очень трудоемкий процесс. Это обусловлено тем, что необходимо предусмотреть широкий спектр возможных традиционных и *нетрадиционных*[3] *угроз и средств, способных им противодействовать [13].*

С появлением сетевых структур и внедрением интернет-технологий возможными причинами отказов и сбоев в работе аппаратно-программных средств стали не только неисправное техническое (программно-логическое) состояние, но и деструктивные действия злоумышленников с целью несанкционированного по-

[3] Начиная с 70-х гг. прошлого века несанкционированный доступ к привилегированной информации осуществляется, как правило, по так называемым скрытым каналам (covert channel), эффективная защита от которого представляется крайне затруднительной. См.: ГОСТ Р 53113.1-2008. Информационная технология. Защита ИТ и АС от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Ч. 1. Общие положения. М. : Ростехрегулирование, 2008. 24 с.; ГОСТ Р 53113.2-2009. Информационная технология. Защита ИТ и АС от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Ч. 2. Рекомендации по организации защиты. М. : Ростехрегулирование, 2009. 26 с.

[1] ***Бурый Алексей Сергеевич,*** *доктор технических наук, эксперт Российской академии наук, директор департамента ФГБУ «Российский институт стандартизации», г. Москва, Российская Федерация.*

E-mail: a.s.burij@gostinfo.ru

[2] ***Усцелемов Вячеслав Николаевич,*** *научный сотрудник, соискатель ФГБУ «Российский институт стандартизации», г. Москва, Российская Федерация.*

E-mail: ustselemov@mail.ru

лучения информации или ее уничтожения, изменения и др. С этим связано обеспечение информационной безопасности как механизма «защиты конфиденциальности, целостности и доступности информации»[4]. Организационные и технические меры защиты информации, реализованные в рамках системы (подсистемы) информационной безопасности (ПИБ), например, АСУ технологическими процессами (ТП), должны быть направлены на обеспечение конфликтной устойчивости [9] и исключение [4]: неправомерного доступа, копирования, модифицирования информации, неправомерного блокирования информации.

Практически безграничные возможности глобальной телематической сети Интернет подтверждают глобальную угрозу виртуальных преступлений, кибертерроризма, а широкое использование информационно-коммуникационных технологий (ИКТ) делают информационные ресурсы наиболее привлекательной целью подобных действий [1].

Основываясь на целевых задачах информационных систем, будем понимать под *информационной безопасностью* свойство объекта (субъекта), характеризующее степень защищенности его потребностей и интересов в качественной (ценной) информации, необходимой ему для устойчивого функционирования и развития (обучения, анализа данных и др.) [13].

Наличие «противоречия» между требованиями по защите информации и открытостью государственных данных, обеспечения их целостности и доступности лишь на первый взгляд выступают в роли именно «противоречия». *Открытость* предполагает возможность при выполнении ряда пользовательских условий получения, внесения изменений и иных действий в открытых информационных ресурсах [15], осуществляя конфиденциальный *электронный документооборот* [12] с использованием электронной цифровой подписи и др., реализуемых в составе российского сегмента сети Интернет, обеспечения информационной безопасности государственных систем, например, Государственной автоматизированной системы РФ «Правосудие» [13].

Необходимость выявления действий злоумышленников на ранней стадии, предотвращая возможные атаки, привела к разработке *систем автоматизированного мониторинга* [2] событий информационной безопасности, ведения киберразведки, фиксации инцидентов безопасности для обучения ПИБ, основываясь в том числе и на *индикаторах компрометации*[5], сигнализирующих, что атака произошла и необходимо проверить ее последствия [16]. Создание базы ранее выявленных случаев преднамеренных воздействий (прецедентов) или атак и их попыток позволяет каждый раз анализировать новые воздействия на предмет того, являются ли они некоторым «повторением прошлого» [17, 21], повышая качество обнаружения атак и их предупреждения.

Интеграция данных и знаний в информационных системах выступают доминантой развития ИКТ, киберфизических систем как на уровне отдельной системы, например, локальной эргатической системы [3, 13], так и на уровне крупномасштабных систем (на примере «системы систем», в качестве которой можно рассматривать информационные структуры «умного города» [3, 4]), автоматизированных телематических сетей в контурах управления сложными динамическими объектами [13, 18] и поддержки принятия решений в них [22].

Предметной целью данного исследования является развитие адаптивных механизмов подсистемы информационной безопасности в организационных системах поддержки принятия решений на основе метода вывода по прецедентам, а также оценки динамики информационного конфликтного взаимодействия, отличающейся возможностью выработки управляющего воздействия для настройки (перенастройки) механизмов подсистемы информационного обмена, на основе оценки возможности сохранения целостности информационных ресурсов различного уровня.

Анализ угроз информационной безопасности

Для анализа угроз информационной безопасности будем исходить из того, что воздействие угроз изменяет состояние распределенной информационной системы (РИС), которое может проявляться в изменении ее количественных или качественных показателей.

Состояние информационной системы в каждый момент времени можно представить вектором $x(t)$ переменных. Разделим все множество состояний РИС на множество $D(t)$ безопасных состояний и множество $N(t)$ небезопасных состояний, т.е. $x(t) = D(t) \cup N(t)$.

Безопасное состояние РИС — это состояние[6], при котором значения параметров системы не выходят из диапазона значений, принятых как безопасные для конкретной РИС.

Небезопасное состояние РИС — это состояние РИС, характеризующееся критичными изменениями значений ее параметров, которые могут привести к преодолению нарушителем подсистемы защиты.

Тогда одной из основных функций подсистемы защиты является поддержание значений вектора $x(t)$ в области допустимых состояний $D(t)$. Появление пограничных и небезопасных состояний РИС, когда вектор $x(t) \notin D(t)$, связано с рисками деструктивных воздействий на РИС.

[4] ГОСТ Р ИСО/МЭК 25010-2015. Информационные технологии. Системная и программная инженерия. Требования и оценка качества систем и программного обеспечения (SQuaRE). Модели качества систем и программных продуктов (Введ. 2015-05-29).

[5] Индикаторы компрометации (*indicators of compromise, IoC*) — технические данные, которые можно использовать для идентификации действий или инструментов атакующих (например, имена хостов, доменные имена, IP-адреса и др.).

[6] Пункт 3.1.2 ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения (Введ. 2009-01-10).

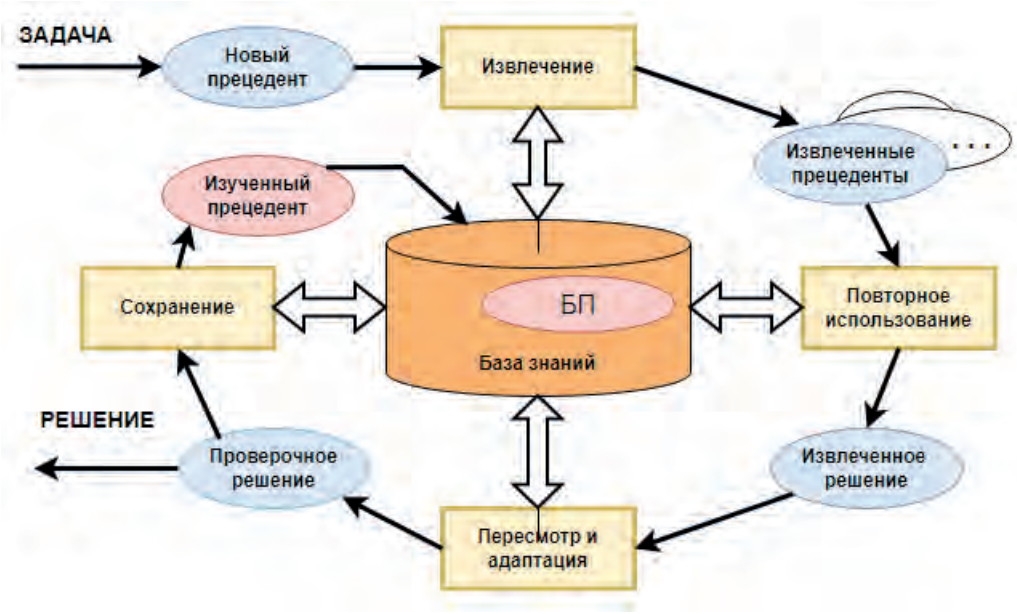

Рис. 1. Структура CBR- цикла рассуждений по прецедентам

Для повышения эффективности функционирования ПИБ целесообразно обеспечивать ее *адаптивную настройку*. Одним из решений указанной задачи является использование при построении и дальнейшей эксплуатации ПИБ формально-логических моделей, позволяющих на основе изменения значений ее параметров оценивать *риск* воздействия угрозы, на основе чего осуществлять настройку механизмов ПИБ.

Проведенный анализ показал [7, 17], что задачи рассматриваемого класса достаточно эффективно решаются на основе использования *методов правдоподобного вывода*, которые позволяют найти рациональное решение в условиях заданных ограничений. Достоинствами указанных методов являются: возможность использования опыта, накопленного системой без интенсивного привлечения экспертов, возможность сокращения времени поиска решения за счет использования уже имеющего решения подобной задачи, возможность применения эвристик, повышающих эффективность процесса поиска решений.

Оценка информационных рисков на основе рассуждений по прецедентам

В основе применения «методов правдоподобного вывода» лежит идея построения «модели рассуждений по прецедентам» (CBR — Case Based Reasoning) [7, 23]. Модели рассуждений являют собой развитие идей логического вывода, решавших подобные задачи в прошлом, применяемые в экспертных системах.

Данный *концептуально-методический подход* позволяет решать новую задачу на основе использования или адаптации решения известной подобной задачи, т. е. использовать опыт, накопленный в решении таких задач.

Методы рассуждений на основе прецедентов включают четыре основных этапа, образующих так называемый *CBR*-цикл, структура которого представлена на *рис*. 1.

Основными этапами *CBR*-цикла являются [20]:

- извлечение наиболее релевантных прецедентов для текущей ситуации из *библиотеки прецедентов* (БП);
- повторное использование извлеченного прецедента для попытки решения текущей задачи;
- пересмотр и адаптация в случае необходимости полученного решения применительно к условиям текущей проблемной ситуации;
- сохранение вновь принятого решения как части нового прецедента.

К *преимуществам* рассуждений на основе прецедентов можно отнести [7]:

- самостоятельность выработки решений в критической ситуации без участия эксперта на основе накопленного опыта;
- сокращение времени поиска решения путем использования уже имеющегося решения для аналогичной задачи;
- накопление ошибочного опыта и исключение подобных действий в будущем: за счет использования ключевых знаний и особенностей (из *базы данных и знаний* рассматриваемой предметной области [11]) можно избежать углубленного изучения всех имеющихся предметных знаний;
- возможность использования эвристик, способствующих росту эффективности поиска прецедентов (так решения, не уникальные для конкретной ситуации, могут быть использованы в других случаях);
- прецеденты представляются в различном виде: от записей в базах данных до предикатов и фреймов.

К *недостаткам* рассуждений на основе прецедентов можно отнести:

– снижение эффективности поиска при избыточном объеме базы прецедентов;
– сложность процесса определения критериев для индексации и сравнения прецедентов.

В большинстве источников под *прецедентом* понимают случай, который имел место ранее и служит примером или оправданием для подобных случаев в дальнейшем [7, 10, 21]. Поэтому представляется возможным использовать накопленный опыт экспертов при описании небезопасных состояний информационной системы.

Применительно к решаемой задаче *прецедент* — это небезопасное состояние подобной РИС в прошлом, которое могло способствовать преодолению рубежей защиты нарушителями.

Под решением задачи подразумевается определение совокупности таких действий, которые бы позволили снизить *риск* преодоления подсистемы защиты до приемлемого уровня. Указанные действия включают в себя шаги по настройке ПИБ, а также реализацию дополнительных рубежей защиты, если таковые не были реализованы ранее.

В качестве результата применения решения подразумевается снижение значения остаточного *риска* преодоления подсистемы защиты до допустимого уровня, а также возвращение значений параметров системы в поле допустимых (безопасных) значений.

Так как описание состояния информационной системы проводится по совокупности ее параметров, то предлагается прецеденты в базе прецедентов формировать по следующей структуре (*рис.* 2):

– описание задачи (метаданные 1—4, 7, 8);
– решение этой задачи (5, 6, 10);
– результат (обоснованность) применения решения (9, 11).

Следовательно, формальное представление прецедента возможно в следующем виде:

$$P_j = \{x_1, x_2, \dots, x_i, \dots, x_n, r, d, c\},$$

где P_j — прецедент из базы прецедентов; x_i, $i \in \overline{[1,n]}$ — значение i-го параметра информационной системы, описывающего ее состояние на момент сохранения прецедента; r — уровень риска преодоления подсистемы защиты нарушителем для указанных в прецеденте значений параметров РИС; d — управляющее воздействие по настройке ПИБ; c — затраты на реализацию управляющего воздействия.

Всё множество известных, а также новых прецедентов в базе прецедентов распределено по принадлежности между соответствующими классами угроз.

Формально можно определить библиотеку прецедентов (БП) в следующем виде:

$$BP = \langle K_1, K_2, \dots, K_m \rangle,$$

где $\{K_k\}$, $k \in \overline{[1,m]}$ — множества классов угроз.

При этом:

$$K_k = \{\langle P_1, P_2, \dots, P_j, \dots, P_n \rangle, do\},$$

где K_k — наименование класса k-й угрозы; P_j — подмножество прецедентов; do — совокупность настроек ПИБ.

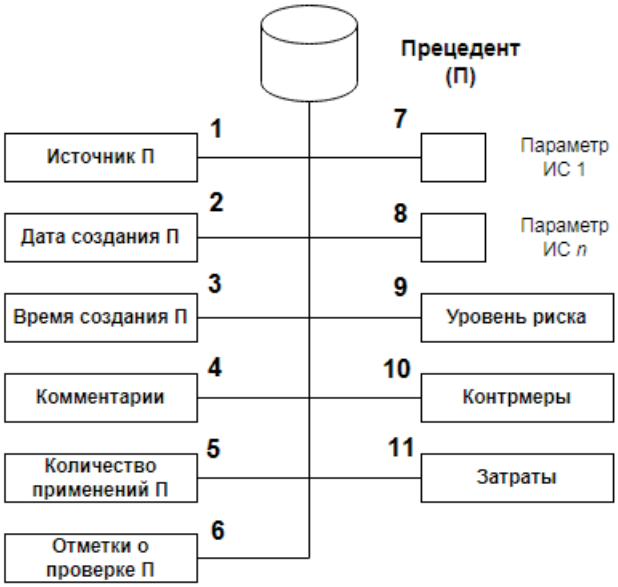

Рис. 2. Структура метаданных прецедента — события атаки на информационную систему

Тогда формальное описание оценки информационных рисков с использованием рассуждений на основе прецедентов можно представить следующим образом [7, 17]:

$$PS = \langle BP, A(p), I^p \rangle,$$

где BP — библиотека (база) прецедентов; $A(p)$ — алгоритм определения сходства прецедентов p; I^p — интерпретатор прецедентов.

Интерпретатор I^p, используя алгоритм $A(p)$, обрабатывает информацию, хранящуюся в базе прецедентов BP, и представляет последовательности процессов:

$$I^p = \langle I^{p1}, I^{p2}, I^{p3}, I^{p4} \rangle,$$

где индексы $p1, \dots, p4$ соответствуют последовательности алгоритмов обнаружения, адаптации, пересмотра и сохранения.

Известны следующие *методы поиска сходства* (подобия прецедентов) [7, 8]: метод ближайшего соседа, метод извлечения прецедентов на основе деревьев решений, метод извлечения прецедентов на основе знаний, метод извлечения прецедентов с учетом их применимости и др. [7, 19].

Проведенный анализ показал, что наиболее целесообразно для решения поставленной задачи использовать метод *k*-взвешенных ближайших соседей, который относится к метрическим методам *классификации* [14]. *Достоинством* метода является наличие более эффективных результатов поиска необходимого решения по сравнению с другими.

Формализация задачи классификации прецедентов

Математическую постановку задачи классификации в общем случае можно представить следующим образом.

Пусть X — множество описаний объектов, *Y* — конечное множество номеров классов. Существует неизвестная целевая зависимость — отображение

$$y^*: X \to Y, \quad (1)$$

значения которой известны только на объектах конечной обучающей выборки $X_m = \{(x_1, y_1), \ldots, (x_m, y_m)\}$.

Требуется построить алгоритм $a: X \to Y$, способный классифицировать, т. е. отнести произвольный объект $x \in X$ к классу $y \in Y$.

Для применения метода ближайшего соседа данная задача сводится к следующему виду (метод модифицирован применительно к решаемой задаче):

– пусть на множестве объектов X задана функция расстояния (метрика)

$$\rho: X \times X \to [0, \infty);$$

– существует целевая зависимость (1), значения которой известны только на объектах обучающей выборки $X^l = (x_1, y_1)_{i=1}^l, y_i = y^*(x_i)$.

Чтобы сгладить влияние выбросов, применяют алгоритм k-взвешенных ближайших соседей, тогда объект u относится к тому классу, элементы которого оказываются больше влияния среди k ближайших соседей $x_u^{(i)}, i = 1, \ldots, k$.

Тогда постановка задачи выглядит следующим образом:

$$w(i,u) = [i \le k];\ a(u; X^l, k) = \quad (2)$$
$$= arg \max_{y \in Y} \sum_{i=1}^k \left[y_u^{(i)} = y\right] w_i,$$

где u — исследуемый объект; $w(i,u)$ — весовая функция; $a(u; X^l, k)$ — алгоритм, строящий локальную аппроксимацию выборки X^l; $y_u^{(i)} = y^*$ — искомое решение.

Процесс поиска прецедентов с использованием модифицированного метода k-взвешенных ближайших соседей заключается в вычислении степени удаленности между значениями параметров, описывающих текущую ситуацию, и извлеченным прецедентом (или в определении степени их близости) [19]. В данной процедуре используется покоординатное сопоставление, так что каждый параметр, описывающий прецедент, рассматривается как одна из координат вектора x. Модификация метода состоит в учете (при поиске прецедентов) предпочтений L_s лица, принимающего решение (ЛПР).

В результате для поиска прецедента определяется расстояние ΔS между текущей ситуацией и прецедентом из базы прецедентов:

$$\Delta S = \left(\sum_{i=1}^n \left(w_i \times SIM\left(x_i^l; x_i^k\right) \times L_i\right)\right) / \sum_{i=1}^n w_i, \quad (3)$$

где w_i — весовое значение (значимость) *i*-го параметра; $SIM\left(x_i^l; x_i^k\right)$ — функция сходства; $x_i^l; x_i^k$ — значения *i*-го параметра в текущем *l* и прошлом *k* прецедентах соответственно; L_i — предпочтение ЛПР по *i*-му показателю прецедента.

Степень сходства прецедентов $x_i^l; x_i^k$ по общему числу параметров N вычисляется по метрике Евклида [19]:

$$SIM\left(x_i^l; x_i^k\right) = \sqrt{\sum_{i=1}^N \left(x_i^l - x_i^k\right)^2}.$$

Данный метод позволяет обеспечивать реализацию эффективного поиска с различной размерностью исходных данных. В случае отсутствия явных значений параметров x_i, описывающих прецедент, или отсутствия недостающих параметров в выбранном прецеденте используются оценки экспертов (после соответствующей обработки). Наиболее прагматичным экспертным методом в данном случае является метод конкордации, так как он позволяет учесть компетентность, ангажированность, взаимозависимость и другие характеристики экспертов, определяющих качество экспертизы. При этом выполнение любого эксперимента предполагает известными измеренные значения выходных параметров системы и перечень факторов, оказывающих влияние на величину выходного параметра.

Направлением развития методов классификации прецедентов является *сочетание* метрических методов с методами экспертного оценивания, что вполне допустимо при задействовании ряда метрик, отличных от евклидового расстояния. В частности, применение к оценке рисков информационной безопасности и настройки ПИБ *риск-ориентированного подхода* на основе ансамблевой нейросети позволяет повысить точность систем поддержки принятия решений по сравнению с ординарной нейросетью за счет использования для решения одной и той же задачи нескольких нейросетей с различными значениями погрешностей отклонений от истинного результата [17].

Заключение

Таким образом, в рамках предложенного концептуально-методического подхода к построению гибридных процедур формирования баз прецедентов разработана формально-логическая модель настройки подсистемы информационной безопасности на основе рассуждений по прецедентам с использованием модифицированного (применительно к решаемой задаче) метода *k*-ближайших соседей. Обоснована рациональная структура базы данных прецедентов и разработан эффективный алгоритм поиска прецедентов. Реализацию эффективного поиска с различной размерностью исходных данных позволил обеспечить модифицированный метод на основе применения процедур классификации на этапе идентификации прецедентов.

Одним из направлений дальнейших исследований предполагается разработка онтологических структур библиотек прецедентов на основе агентных управляющих систем, что позволит, по мнению авторов, существенно расширить возможности методов классификации прецедентов, обеспечивая кроссплатформенность построения баз прецедентов для междисциплинарных предметных областей.

Рецензент: ***Бетанов Владимир Вадимович,*** *доктор технических наук, профессор, заслуженный деятель науки Российской Федерации, академик РАРАН, начальник центра АО «Российские космические системы», г. Москва, Российская Федерация.*
E-mail: vlavab@mail.ru

Литература

1. Емельянов В.А., Пастухова С.Е., Соболев А.С., Кучеренко В.А. Алгоритмы кибербезопасности правдоподобно дескрипционной логики в динамических системах // Изв. Тульского гос. ун-та. Технические науки. 2023. № 4. С. 15—22.
2. Бурый А.С. Структуризация систем мониторинга информационных ресурсов // Правовая информатика. 2023. № 1. С. 52—61. DOI: 10.21681/1994-1404-2023-1-52-61 .
3. Бурый А.С., Ловцов Д.А. Информационные структуры умного города на основе киберфизических систем // Правовая информатика. 2022. № 4. С. 15—26. DOI: 10.21681/1994-1404-2022-4-15-26 .
4. Бурый А.С., Ловцов Д.А. Информационные технологии цифровой трансформации умных городов // Правовая информатика. 2022. № 2. С. 4—13. DOI: 10.21681/1994-1404-2022-2-04-13 .
5. Бурый А.С., Усцелемов В.Н. Онтологический подход к формированию когнитивных моделей оценки кибербезопасности // Информационно-экономические аспекты стандартизации и технического регулирования. 2020. № 3 (55). С. 77—84.
6. Бурый А.С., Усцелемов В.Н. Информационная безопасность автоматизированных систем // Информационно-экономические аспекты стандартизации и технического регулирования. 2023. № 2 (72). С. 31—37.
7. Варшавский П.Р., Ар Кар Мьо, Шункевич Д.В. Применение методов классификации и кластеризации для повышения эффективности работы прецедентных систем // Программные продукты и системы. 2017. № 4. С. 625—631.
8. Дойникова Е.В., Чечулин А.А., Котенко И.В. Оценка защищенности компьютерных сетей на основе метрик CVSS // Информационно-управляющие системы. 2017. № 6 (91). С. 76—87. DOI: 10.15217/issn1684-8853.2017.6.76 .
9. Жидко Е.А., Разиньков С.Н. Модель подсистемы безопасности и защиты информации системы связи и управления критически важного объекта // Системы управления, связи и безопасности. 2018. № 1. С. 122—135.
10. Крылов А.В. Проблема извлечения знаний с использованием рассуждений на основе прецедентов // Изв. вузов. Приборостроение. 2018. Т. 61. № 11. С. 956—962.
11. Ловцов Д.А. Информационная теория эргасистем : монография. М. : РГУП, 2021. 314 с. ISBN 978-5-93916-887-8.
12. Ловцов Д.А. Проблемы правового регулирования электронного документооборота // Информационное право. 2005. № 2. С. 28—31.
13. Ловцов Д.А. Теория защищенности информации в эргасистемах : монография. М. : РГУП, 2021. 273 с. ISBN 978-5-93916-896-0.
14. Ловцов Д.А., Федичев А.В. Архитектура национального классификатора правовых режимов информации ограниченного доступа // Правовая информатика. 2017. № 2. С. 35—54. DOI: 10.21681/1994-1404-2017-2-35-54 .
15. Марков А.С. Правоприменение открытых данных с учетом требований по информационной безопасности // Мониторинг правоприменения. 2017. № 3 (24). С. 86—96. DOI: 10.21681/2412-8163-2017-3-86-96 .
16. Мещеряков Р.В., Исхаков С.Ю. Исследование индикаторов компрометации для средств защиты информационных и киберфизических систем // Вопросы кибербезопасности. 2022. № 5 (51). С. 82—99. DOI: 10.21681/2311-3456-2022-5-82-99 .
17. Усцелемов В.Н. Совершенствование подсистемы информационной безопасности на основе интеллектуальных технологий // Прикладная информатика. 2016. Т. 11. № 3 (63). С. 31—38.
18. Фомичева С.Г. Влияние ранжирования индикаторов атак на качество моделей машинного обучения в агентных системах непрерывной аутентификации // T-Comm: Телекоммуникации и транспорт. 2023. Т. 17. № 8. С. 45—55. DOI: 10.36724/2072-8735-2023-17-8-45-55 .
19. Шелухин О.И., Ерохин С.Д., Полковников М.В. Технологии машинного обучения и сетевой безопасности. М. : Горячая линия-Телеком, 2021. 360 с. ISBN 978-5-9912-0913-7.
20. Юдин В.Н., Карпов Л.Е. Модель поведения объектов, подверженных спонтанному изменению в прецедентном подходе к управлению // Труды ИСП РАН. 2016. Т. 28. Вып. 4. С. 183—192. DOI: 10.15514/ISPRAS-2016-28 (4)-11 .
21. Jung J. W., Lee S. W. Security requirement recommendation method using case-based reasoning to prevent advanced persistent threats. Applied Sciences. 2023. Vol. 13. No. 3. P. 1505.
22. Kim D., Jeong D., Seo Y. Intelligent Design for Simulation Models of Weapon Systems Using a Mathematical Structure and Case-Based Reasoning. Applied Sciences. 2020. No. 10 (21). P. 7642. DOI: 10.3390/app10217642 .
23. San Zaw K., Vasupongayya S. A case-based reasoning approach for automatic adaptation of classifiers in mobile phishing detection. Journal of Computer Networks and Communications. 2019. Vol. 2019. Art. ID 7198435. DOI: 10.1155/2019/7198435 .

DEVELOPING PRECEDENT-BASED DECISION SUPPORT SYSTEMS IN DISTRIBUTED INFORMATION STRUCTURES

Aleksei Buryi, *Dr.Sc. (Technology), expert at the Russian Academy of Sciences, Department Director at the Russian Standardisation Institute, Moscow, Russian Federation.*
E-mail: a.s.burij@gostinfo.ru

Viacheslav Ustselemov, *Researcher, external Ph.D. student at the Russian Standardisation Institute, Moscow, Russian Federation.*
E-mail: ustselemov@mail.ru

Keywords: *distributed information system, precedent, information security, risk, decision support, case-based reasoning system, classifier, method, model, algorithm, similarity.*

Abstract

Purpose of the work: developing adaptive mechanisms for the information security subsystem in organisational decision support systems using the precedent-based method for building conclusions as well as evaluating the dynamics of information conflict interaction with the ability to developing control actions for (re)adjusting the mechanisms of the information exchange subsystem.

Methods used: a complex use of system and comparative analysis, methods ensuring information security, the precedent-based method for building reasoning, and logical concept justification of structures for building distributed information systems.

Study findings: justification is given for a conceptual and methodological approach to building hybrid procedures for forming precedent databases based on the CBR (Case-Based Reasoning) method, a combination of metric methods for classifying information security incidents and algorithms for expert evaluation of classification objects in tasks of monitoring information resources of integrated information structures of a given subject area. A formal logic model is developed for adjusting the information security subsystem based on precedent-based reasoning using a modified k-nearest neighbours method. A rational structure for the precedent database and an efficient algorithm for precedent search are justified.

References

1. Emel'ianov V.A., Pastukhova S.E., Sobolev A.S., Kucherenko V.A. Algoritmy kiberbezopasnosti pravdopodobno deskriptsionnoi logiki v dinamicheskikh sistemakh. Izv. Tul'skogo gos. un-ta. Tekhnicheskie nauki, 2023, No. 4, pp. 15–22.
2. Buryi A.S. Strukturizatsiia sistem monitoringa informatsionnykh resursov. Pravovaia informatika, 2023, No. 1, pp. 52–61. DOI: 10.21681/1994-1404-2023-1-52-61 .
3. Buryi A.S., Lovtsov D.A. Informatsionnye struktury umnogo goroda na osnove kiberfizicheskikh sistem. Pravovaia informatika, 2022, No. 4, pp. 15–26. DOI: 10.21681/1994-1404-2022-4-15-26 .
4. Buryi A.S., Lovtsov D.A. Informatsionnye tekhnologii tsifrovoi transformatsii umnykh gorodov. Pravovaia informatika, 2022, No. 2, pp. 4–13. DOI: 10.21681/1994-1404-2022-2-04-13 .
5. Buryi A.S., Ustselemov V.N. Ontologicheskii podkhod k formirovaniiu kognitivnykh modelei otsenki kiberbezopasnosti. Informatsionno-ekonomicheskie aspekty standartizatsii i tekhnicheskogo regulirovaniia, 2020, No. 3 (55), pp. 77–84.
6. Buryi A.S., Ustselemov V.N. Informatsionnaia bezopasnost' avtomatizirovannykh sistem. Informatsionno-ekonomicheskie aspekty standartizatsii i tekhnicheskogo regulirovaniia, 2023, No. 2 (72), pp. 31–37.
7. Varshavskii P.R., Ar Kar M'o, Shunkevich D.V. Primenenie metodov klassifikatsii i klasterizatsii dlia povysheniia effektivnosti raboty pretsedentnykh sistem. Programmnye produkty i sistemy, 2017, No. 4, pp. 625–631.
8. Doinikova E.V., Chechulin A.A., Kotenko I.V. Otsenka zashchishchennosti komp'iuternykh setei na osnove metrik CVSS. Informatsionno-upravliaiushchie sistemy, 2017, No. 6 (91), pp. 76–87. DOI: 10.15217/issn1684-8853.2017.6.76 .
9. Zhidko E.A., Razin'kov S.N. Model' podsistemy bezopasnosti i zashchity informatsii sistemy sviazi i upravleniia kriticheski vazhnogo ob"ekta. Sistemy upravleniia, sviazi i bezopasnosti, 2018, No. 1, pp. 122–135.
10. Krylov A.V. Problema izvlecheniia znanii s ispol'zovaniem rassuzhdenii na osnove pretsedentov. Izv. vuzov. Priborostroenie, 2018, t. 61, No. 11, pp. 956–962.
11. Lovtsov D.A. Informatsionnaia teoriia ergasistem : monografiia. M. : RGUP, 2021. 314 pp. ISBN 978-5-93916-887-8.

12. Lovtsov D.A. Problemy pravovogo regulirovaniia elektronnogo dokumentooborota. Informatsionnoe pravo, 2005, No. 2, pp. 28–31.
13. Lovtsov D.A. Teoriia zashchishchennosti informatsii v ergasistemakh : monografiia. M. : RGUP, 2021. 273 pp. ISBN 978-5-93916-896-0.
14. Lovtsov D.A., Fedichev A.V. Arkhitektura natsional'nogo klassifikatora pravovykh rezhimov informatsii ogranichennogo dostupa. Pravovaia informatika, 2017, No. 2, pp. 35–54. DOI: 10.21681/1994-1404-2017-2-35-54 .
15. Markov A.S. Pravoprimenenie otkrytykh dannykh s uchetom trebovanii po informatsionnoi bezopasnosti. Monitoring pravoprimeneniia, 2017, No. 3 (24), pp. 86–96. DOI: 10.21681/2412-8163-2017-3-86-96 .
16. Meshcheriakov R.V., Iskhakov S.Iu. Issledovanie indikatorov komprometatsii dlia sredstv zashchity informatsionnykh i kiberfizicheskikh sistem. Voprosy kiberbezopasnosti, 2022, No. 5 (51), pp. 82–99. DOI: 10.21681/2311-3456-2022-5-82-99 .
17. Ustselemov V.N. Sovershenstvovanie podsistemy informatsionnoi bezopasnosti na osnove intellektual'nykh tekhnologii. Prikladnaia informatika, 2016, t. 11, No. 3 (63), pp. 31–38.
18. Fomicheva S.G. Vliianie ranzhirovaniia indikatorov atak na kachestvo modelei mashinnogo obucheniia v agentnykh sistemakh nepreryvnoi autentifikatsii. T-Comm: Telekommunikatsii i transport, 2023, t. 17, No. 8, pp. 45–55. DOI: 10.36724/2072-8735-2023-17-8-45-55 .
19. Shelukhin O.I., Erokhin S.D., Polkovnikov M.V. Tekhnologii mashinnogo obucheniia i setevoi bezopasnosti. M. : Goriachaia liniia-Telekom, 2021. 360 pp. ISBN 978-5-9912-0913-7.
20. Iudin V.N., Karpov L.E. Model' povedeniia ob"ektov, podverzhennykh spontannomu izmeneniiu v pretsedentnom podkhode k upravleniiu. Trudy ISP RAN, 2016, t. 28, vyp. 4, pp. 183–192. DOI: 10.15514/ISPRAS-2016-28 (4)-11 .
21. Jung J. W., Lee S. W. Security requirement recommendation method using case-based reasoning to prevent advanced persistent threats. Applied Sciences. 2023. Vol. 13. No. 3. P. 1505.
22. Kim D., Jeong D., Seo Y. Intelligent Design for Simulation Models of Weapon Systems Using a Mathematical Structure and Case-Based Reasoning. Applied Sciences. 2020. No. 10 (21). P. 7642. DOI: 10.3390/app10217642 .
23. San Zaw K., Vasupongayya S. A case-based reasoning approach for automatic adaptation of classifiers in mobile phishing detection. Journal of Computer Networks and Communications. 2019. Vol. 2019. Art. ID 7198435. DOI: 10.1155/2019/7198435 .