УДК 004.4

Д.Е. Пальчунов

Институт математики СО РАН им. С.Л. Соболева
пр. Копьюга, 4, Новосибирск, 630090, Россия
Новосибирский государственный университет
e-mail: palch@math.nsc.ru

Г.Э. Яхъяева
Новосибирский государственный университет
ул. Пирогова, 2, Новосибирск, 630090, Россия
e-mail: gulnara@math.nsc.ru

А.А. Хамутская
Новосибирский государственный университет
ул. Пирогова, 2, Новосибирск, 630090, Россия
e-mail: alena.khamutskaya@gmail.com

ПРОГРАММНАЯ СИСТЕМА УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ РИСКАМИ RiskPanel[1]

Аннотация: В настоящей статье рассмотрены современные подходы к оценке рисков неблагоприятных событий, необходимость в которых возникает при обеспечении информационной безопасности корпоративной информационной системы. Проведён анализ существующих программных систем, предназначенных для оценки таких рисков. Предложен подход к анализу рисков, основанный на построении формальных моделей прецедентов компьютерных атак. Изложены математические основы предлагаемого подхода. Описана программная реализация подхода – программная система RiskPanel.

Ключевые слова: информационная безопасность, компьютерная атака, управление рисками, корпоративная информационная система, нечёткие модели.

[1] Работа выполнена при поддержке гранта Федерального агентства по образованию, государственный контракт П-1008, а так же междисциплинарного интеграционного проекта фундаментальных исследований СО РАН 119.

1. Обзор инструментальных средств управления информационными рисками

В настоящее время актуальность эффективного управления рисками в сфере информационной безопасности трудно переоценить [1]. В отчётах крупных компаний часто фигурируют огромные цифры финансовых потерь, понесенных в результате хакерской атаки, утраты ценных сведений и т.п.

Основная задача специалистов, обеспечивающих компьютерную безопасность – это оперативная реакция на изменения текущего статуса защищенности всех компонент корпоративной информационной системы. Для этой цели полезно иметь программную систему, позволяющую без необходимости приобретения особых навыков оперативно определить тип атаки, узнать самую свежую информацию о возможных последствиях атак и способах их предотвращения. На настоящее время разработано более сотни различных программных систем управления информационными рисками. Все их можно условно разделить на две группы [2-4]:

- программные системы базового уровня – методики качественного анализа рисков;
- программные системы полного анализа – методики количественного анализа рисков.

Программные системы базового уровня, как правило, используются компаниями, находящимися на уровне 3 зрелости по классификации CMM [5]. К методикам качественного анализа рисков на основе требований ISO 17999 относятся методики COBRA и RA Software Tool.

COBRA. Во второй половине 90-х годов компания C&A Systems Security Ltd. разработала методику и инструментарий для анализа и управления информационными рисками под названием COBRA [6]. Эта методика позволяет в автоматизированном режиме выполнить достаточно простой вариант оценивания информационных рисков любой компании. Анализ рисков, выполняемый данным методом, отвечает базовому уровню безопасности. Достоинство методики – в ее простоте. Необходимо ответить на несколько десятков вопросов, затем автоматически формируется отчет.
RA Software Tool [7]. Методика базируется на британском стандарте BS 7799 и на методических материалах Британского института стандартов.

К программным системам полного анализа рисков относится инструментарий с более развитыми средствами анализа рисков и управления ими. Такой инструментарий пользуется спросом у организаций, находящихся на 4-м и 5-м уровнях зрелости по классификации CMM. На четвертом уровне для руководства организации актуальны вопросы измерения параметров, характеризующих режим информационной безопасности. Технология управления режимом информационной безопасности остается прежней, но на этапе анализа рисков применяются количественные методы, позволяющие оценить параметры остаточных рисков, эффективность различных вариантов контрмер при управлении рисками. На пятом уровне ставятся и решаются различные варианты оптимизационных задач в области обеспечения режима информационной безопасности. Рассмотрим самые известные программные системы данного класса.

CRAMM. Метод CRAMM (CCTA Risk Analysis and Management Method) [8] был разработан Агентством по компьютерам и телекоммуникациям Великобритании (Central Computer and Telecommunications Agency) по заданию Британского правительства и взят на вооружение в качестве

государственного стандарта. Он используется, начиная с 1985 г. правительственными и коммерческими организациями Великобритании.
Исследование информационной безопасности системы с помощью CRAMM проводится в несколько этапов. На первом этапе производится формализованное описание границ информационной системы, ее основных функций, категорий пользователей, а также персонала, принимающего участие в обследовании. На втором этапе описывается и анализируется все, что касается идентификации и определения ценности ресурсов системы. По завершению данного этапа заказчик имеет качественное описание уровня информационной безопасности своей компании.

Следующий этап позволяет оценить риски либо на основе сделанных оценок угроз и уязвимостей при проведении полного анализа рисков, либо путем использования упрощенных методик для базового уровня безопасности. На последнем этапе производится поиск адекватных контрмер.

RiskWatch. Методика разработана американской компанией RiskWatch Inc [9]. Используемая в программе методика состоит из четырех этапов. На первом этапе описываются параметры организации: ее тип; состав исследуемой системы; базовые требования в области безопасности. Второй этап – внесение данных, касающихся конкретных характеристик системы. Данные могут вводиться вручную или импортироваться из отчетов, созданных инструментальными средствами исследования уязвимости компьютерных сетей. На этом этапе: описываются ресурсы, потери и классы инцидентов; с помощью опросника, база которого содержит более 600 вопросов, выявляются возможные уязвимости; задается частота возникновения каждой из выделенных угроз, степень уязвимости и ценность ресурсов. Третий этап – оценка рисков нарушения безопасности. Четвертый этап – генерация отчетов.

Digital Security Office 2006 – комплексное решение для управления информационной безопасностью, разработанное российской компанией Digital Security [10]. Digital Security Office 2006 включает в себя систему разработки и управления политикой безопасности информационной системы КОНДОР и систему анализа и управления информационными рисками ГРИФ. Система КОНДОР предназначена для обеспечения базового уровня информационной безопасности компании. Система ГРИФ направлена на обеспечение полного анализа информационных рисков. Эта система позволяет проанализировать уязвимости информационной системы и оценить возможный ущерб для компании при реализации потенциальных угроз через найденные уязвимости.

В ходе работы с системой ГРИФ сроятся две модели: модель анализа информационных потоков и модель анализа угроз и уязвимостей. Анализ рисков информационной безопасности осуществляется с помощью построения модели информационной системы организации. Для оценки рисков информационной системы организации защищенность каждого ценного ресурса определяется при помощи анализа угроз, действующих на конкретный ресурс, и уязвимостей, через которые данные угрозы могут быть реализованы.

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) [11] разработана в университете Карнеги-Мелон, США и предназначена для оценки критичных угроз, активов и уязвимостей.

2. Анализ недостатков существующих программных решений

Первым шагом любой методики управления информационными рисками является идентификация рисков, в том числе, их составляющих – угроз и уязвимостей. Типовым подходом к решению данной задачи является

использование различных стандартных списков классов рисков. Компании, разрабатывающие программные системы по информационной безопасности разрабатывают свои списки рисков (угроз и уязвимостей) информационной безопасности или используют некоторые общепринятые стандарты, либо покупают такие списки у крупных производителей программного обеспечения. В частности, используются каталоги стандартных рисков, угроз и уязвимостей. Примером такого каталога является список Common Vulnerabilities and Exposures (CVE) [12] – единый каталог уязвимостей. Трудности реализации такого подхода обусловлены излишней конкретизацией. Заказчик, используя подробные каталоги, может «потонуть» в море рисков, которые система для него идентифицирует.

Вторая трудность, с которой сталкиваются разработчики систем информационной безопасности, это очень динамичное развитие информационных технологий, и, как следствие, непрерывное появление новых угроз и уязвимостей. Разработчики стараются отслеживать появление новых рисков, выпускают новые версии программ. Для решения этой задачи программная система RiskPanel, которая подробно будет описана в третьем параграфе, имеет модуль полуавтоматического пополнения базы данных прецедентов компьютерных атак, которое осуществляется за счёт анализа оперативной информации, представленной в Интернет и других источниках [13-16].

Третья трудность, с которой сталкиваются разработчики современных программных решений, связанна с методологией и техникой оценки рисков нарушения информационной безопасности. В каждой программной системе по управлению информационными рисками заложен некий алгоритм качественной или количественной оценки идентифицированных рисков. Как правило, этот алгоритм является «ноу-хау» компании и является скрытым для тех, кто не вовлечен в разработку данной программной системы.

Заказчик, работая с предоставленной ему программной системой по информационной безопасности, получает оценку определённого набора рисков и список контрмер, которые необходимо предпринять для ликвидации данных рисков. Однако у него нет возможности восстановить знания о тех прецедентах – конкретных случаях компьютерных атак, на основании которых были получены данные оценки. Теоретические принципы и конкретные математические формулы, на основе которых производится оценка рисков, являются «ноу-хау» разработчиков программных систем и, соответственно, недоступны пользователю. Как следствие для пользователя программная система представляет собой «чёрный ящик», который выдаёт рекомендации, но аргументация этих рекомендаций, информация, которая стоит за полученными выводами, является недоступной. В результате пользователю, во-первых, сложно оценить достоверность сведений о рисках, и, во-вторых, нет полного понимания, что дальше делать с полученной информацией.

В предлагаемом нами подходе вся исходная информация о прецедентах компьютерных атак хранится в базе знаний системы и, при соответствующем запросе заказчика, становится ему доступной. Более того, при пополнении базы знаний, создаются новые классы рисков, и система в автоматическом режиме находит необходимые контрмеры для ликвидации этих рисков.

3. Математические основы разрабатываемого подхода

Как было описано выше, существующие программные средства оценки рисков неблагоприятных событий, которые выявляются при обеспечении безопасности информационных систем, имеют определённые недостатки. Один из таких недостатков состоит в том, что при их применении пользователь имеет только несколько чисел, характеризующих риски (например, вероятность данного риска, важность этого риска и т.п.), то

остаётся непонятным, что с этими числами делать дальше. Это, в частности, связано с тем обстоятельством, что содержательная информация, которая представлена за этими числами, недоступна для пользователя. Содержательная информация «спрессована» в числа без возможности её обратного восстановления по этим числам.

Отмеченный выше недостаток можно устранить, если иметь дело не только с итоговыми числами, представляющими, например, вероятность возникновения неблагоприятных событий и степень их критичности, но и с исходной информацией, из которой эти числа получены – с прецедентами реальных компьютерных атак и других видов нарушения информационной безопасности. Для этого необходимо работать с базой данных прецедентов компьютерных атак. Подробное описание программной системы RiskPanel, позволяющей оценивать риски информационной безопасности исходя из имеющихся прецедентов компьютерных атак, будет дано в третьем параграфе. В настоящем разделе изложим математические основы предлагаемого подхода.

Принципиальное отличие математических основ предлагаемого подхода [17, 18] от стандартных методов оценки рисков и методов актуарной математики [19] состоит в том, что здесь работа ведётся не с числовыми оценками возможности срабатывания различных рисков, а с множествами прецедентов, на которых эти риски сработали. Кратко это отличие можно описать следующим образом. При стандартном подходе информация сначала оцифровывается (в другой терминологии фазифицируется), а потом обрабатывается. В рамках предлагаемого подхода вся имеющаяся информация, включающая и описание онтологии предметной области, и эмпирические данные, сначала полностью обрабатывается, и только окончательный результат фазифицируется, превращается в числа из интервала [0, 1]. Такой подход даёт возможность на всех шагах обработки

информации иметь дело с полностью релевантными данными, не искажёнными оцифровкой.

Проиллюстрируем это на примере. Допустим, нужно рассчитать вероятность риска «Неавторизованная модификация информации в базе данных». Предположим, что эта угроза может осуществиться через две различные уязвимости *A* и *B*. В методике компании Digital Security [10], заказчику предлагается рассчитать вероятности реализации угрозы через каждую из уязвимостей: $P(A)$ и $P(B)$. При помощи формулы $P(A \cup B) = 1 - (1 - P(A))(1 - P(B))$ вычисляется общая вероятность реализации угрозы. Например, если $P(A) = 0{,}5$ и $P(B) = 0{,}5$, то $P(A \cup B) = 0{,}75$. При этом не может быть учтена информация о совместимости или несовместимости событий *A* и *B*. Если иметь не только числовые оценки, но и стоящие за ними прецеденты компьютерных атак, то будет известна информация о совместимости данных событий. При этом, если рассматриваемые события несовместимы (т.е. $P(A \cap B) = 0$), то $P(A \cup B) = 1$; если они происходят одновременно, то $P(A \cup B) = 0{,}5$.

В настоящей работе мы рассматриваем конечное множество прецедентов компьютерных атак [1] и, исходя из этих прецедентов, оцениваем вероятности различных утверждений, имеющих отношение к безопасности корпоративной информационной системы. Каждый прецедент формализуется в виде алгебраической системы. Для простоты и удобства рассмотрения, без ограничения общности, можно считать, что у всех алгебраических систем, описывающих прецеденты компьютерных атак, основное множество (с точностью до переобозначения) одно и то же. Также, без ограничения общности, можно считать, что, после соответствующего переобозначения, основные множества алгебраических систем, описывающих прецеденты, не пересекаются.

Таким образом, каждый прецедент компьютерной атаки описывается алгебраической системой $\mathfrak{A} = \langle A, \sigma \rangle$, где A – основное множество алгебраической системы, а σ – её сигнатура. Сигнатура σ – это множество понятий, на языке которых описывается данная предметная область: множество различных уязвимостей, угроз, контрмер, последствий и т.п. Будем считать, что у всех прецедентов компьютерных атак сигнатура одна. Обогатим сигнатуру σ, добавив для каждого элемента a константу c_a: обозначим $\sigma_A = \sigma \cup \{c_a \mid a \in A\}$. Алгебраические системы, с помощью которых описываем экземпляры предметной области, принадлежат классу

$$\mathbb{K}(\sigma_A) \leftrightharpoons \{\mathfrak{A} = \langle \{c_a^{\mathfrak{A}} \mid a \in A\}, \sigma_A \rangle \mid c_a^{\mathfrak{A}} \neq c_b^{\mathfrak{A}} \text{ при } a \neq b\}.$$

Как было отмечено выше, считаем, что для разных $\mathfrak{A}, \mathfrak{B} \in \mathbb{K}(\sigma_A)$ выполняется $|\mathfrak{A}| \cap |\mathfrak{B}| = \emptyset$. Через $\wp(X)$ будем обозначать множество всех подмножеств множества X.

Алгебраическую систему $\mathfrak{A}$, являющуюся моделью некоторой компьютерной атаки, назовем ***прецедентом*** этой предметной области. Для каждого набора прецедентов E определим прецедентную систему $\mathfrak{A}_E$.

Определение 1. *Пусть $E \subseteq \mathbb{K}(\sigma_A)$ – некоторое множество прецедентов.* ***Прецедентной системой*** (*порожденной множеством E*) *назовем алгебраическую систему $\mathfrak{A}_E \leftrightharpoons \langle A, \sigma, \tau_E \rangle$, где $\tau_E : S(\sigma_A) \to \wp(E)$, причем для любого предложения φ сигнатуры σ_A выполнено $\tau_E(\varphi) = \{\mathfrak{A} \in E \mid \mathfrak{A} \models \varphi\}$.*

Заметим, что прецедентная система является частным случаем булевозначной модели [18], в которой значениями истинности предложений являются элементы булевой алгебры. В данном случае значениями истинности предложений являются элементы $\to \wp(E)$ – булевой алгебры всех подмножеств множества E.

Рассмотрим множество X всевозможных компьютерных атак (как уже произошедших и известных нам, так и тех, которые еще могут произойти). Очевидно, что в каждый момент времени наше знание об уже произошедших компьютерных атаках конечно. Однако это знание постоянно растет, пополняясь новыми прецедентами. Таким образом, можно предполагать, что потенциально множество X прецедентов компьютерных атак является счётным. При этом достаточно рассматривать только конечные подмножества множества X, как формализацию нашего знания о предметной области в разные моменты времени. Таким образом, будем рассматривать только конечные множества прецедентов, и, следовательно, только булевозначные модели с конечными булевыми алгебрами. Обозначим

$$\mathbb{K}^f \leftrightharpoons \{\mathfrak{A}_E \mid E \subseteq \mathbb{K}(\sigma_A) \text{ и } \|E\| < \omega\}.$$

Основной целью программной системы по управлению информационными рисками является идентификация и оценивание рисков, связанных с информационной безопасностью корпоративной информационной системы. В большинстве методик управления информационными рисками при их оценивании используются объективные и/или субъективные вероятности [3].

Под **объективной вероятностью** понимается относительная частота появления какого-либо события в общем объеме наблюдений или отношение числа благоприятных исходов к общему количеству наблюдений. Под **субъективной вероятностью** имеется в виду мера уверенности некоторого эксперта или группы экспертов в том, что данное событие в действительности будет иметь место.

В подходе, представленном в настоящей работе, при идентификации и оценивании рисков также будем использовать объективную и субъективную вероятности. В нашем случае объективная вероятность – это функция истинности $\mu(\varphi)$ в нечёткой модели $\mathfrak{A}_\mu$ (которая будет определена ниже), а

субъективная вероятность – это оценка, сделанная экспертом. Опишем сначала методы подсчета объективных вероятностей рисков.

Пусть у нас есть прецедентная модель $\mathfrak{A}_E$, являющаяся математической формализацией базы знаний о прецедентах компьютерных атак. Для того, чтобы вычислить объективные вероятности происхождения тех или иных атак, определим понятие фазификации прецедентной модели.

Определение 2. *Модель* $\mathfrak{A}_\mu = \langle A, \sigma_A, \mu \rangle$ *назовем* ***фазификацией*** *прецедентной модели* $\mathfrak{A}_E \in \mathbb{K}^f$ (*и будем обозначать* $\mathfrak{A}_\mu = Fuz(\mathfrak{A}_E)$), *если для любого предложения* φ *сигнатуры* σ_A *выполнено* $\mu(\varphi) = \frac{\|\tau_E(\varphi)\|}{\|E\|}$. *Будем обозначать* $\mathfrak{A}_\mu \models_\alpha \varphi$, *если* $\mu(\varphi) = \alpha$.

Заметим, что полученная модель является нечеткой моделью, так как ее истинностная функция μ принимает свои значения из интервала $[0,1]$. Обозначим через $\mathbb{K}^\mu \leftrightharpoons \{\mathfrak{A}_\mu \mid \exists \mathfrak{A}_E \in \mathbb{K}^f : \mathfrak{A}_\mu = Fuz(\mathfrak{A}_E)\}$ класс всех фазификаций прецедентных моделей.

Определение 3. *Предложение* φ *называется* ***истинным на фазификации****,* $\mathfrak{A}_\mu$, *если* $\mu(\varphi) = 1$.

Теорема 1. *Предложение* φ *истинно на любой фазификации* $\mathfrak{A}_\mu$ *тогда и только тогда, когда оно тождественно истинно в классической логике предикатов.*

На практике, как правило, нет полной информации о рассматриваемой предметной области. Например, никакой эксперт не обладает информацией обо всех компьютерных атаках и нарушениях информационной безопасности, произошедших на настоящий момент времени. Следовательно,

нет возможности дать полное описание прецедентной модели, описывающей данную предметную область. По этой причине приходится рассматривать класс $K \subseteq \mathbb{K}^{\mu}$ прецедентных моделей, описывающих те свойства предметной области, которые уже известны. Для формального описания такой ситуации введем понятие обобщенной нечеткой модели.

Определение 4. *Пусть* $K \subseteq \mathbb{K}^{\mu}$ *и* $K \neq \emptyset$. *Модель* $\mathfrak{A}_K = \langle A, \sigma_A, \xi_K \rangle$ *назовем* ***обобщенной нечеткой моделью*** (*порожденной классом* K), *если для любого предложения* φ *сигнатуры* σ_A *истинностное значение* $\xi_K(\varphi)$ *является множеством всех объективных вероятностей предложения* φ *на всех моделях класса* K, *т.е. выполнено* $\xi_K(\varphi) = \{\alpha \in [0,1] \mid \exists \mathfrak{A} \in K : \mathfrak{A} \vDash_{\alpha} \varphi\}$.

Поскольку у нас нет достаточного объёма объективной информации, необходимо использовать субъективные вероятности (экспертные оценки) существенных для нас утверждений о предметной области. Пусть U – множество предложений сигнатуры σ_A, про которые известны их субъективные вероятности. Рассмотрим класс $K \subseteq \mathbb{K}^{\mu}$ таких моделей $\mathfrak{A}_{\mu}$, у которых для каждого предложения φ из U значение $\mu(\varphi)$ совпадает со значением субъективной вероятности истинности этого предложения φ. Этот факт означает, что на всех предложениях из U значения субъективной и объективной вероятностей совпадают. Для такого класса K верна следующая теорема.

Теорема 2. *На обобщенной нечеткой модели* $\mathfrak{A}_K = \langle A, \sigma_A, \xi_K \rangle$ *для любого предложения* φ *сигнатуры* σ_A *истинностное значение* $\xi_K(\varphi)$ *является интервалом рациональных чисел.*

Заметим, что кроме совпадения значений $\mu(\varphi)$ на классе K можно также потребовать истинность онтологии предметной области. Однако и при этом

требовании Теорема 2 останется верной: можно считать, что все предложения, входящие в онтологию, входят и во множество U, при этом их субъективная вероятность равна 1. Более подробную информацию по обобщённым нечётким моделям можно найти в [17, 18].

4. Описание системы RiskPanel

Для того чтобы эффективно управлять рисками при обеспечении информационной безопасности подконтрольных систем, необходимо обладать средствами анализа уровня их защищённости, новых видов угроз информационной безопасности и способов их реализации. Представленные на рынке продукты риск-менеджмента в области информационной безопасности основаны на том, что анализ рисков нарушения безопасности ресурсов информационных систем организации производится разово или с низкой периодичностью, например, раз в полгода. При этом проводится лишь довольно общий анализ без учёта того, что ситуация в компании может меняться значительно чаще. Поскольку сфера информационных технологий очень динамична, необходимо проводить анализ рисков постоянно, учитывая происходящие в мире прецеденты нарушения информационной безопасности.

Следующий вопрос – что конкретно пользователь должен делать с информацией о рисках, которую ему выдала программная система? Здесь можно выделить следующие три вопроса и, соответственно, вытекающие из них задачи.

– Во-первых, пользователю необходимо понять, насколько оценка тех или иных рисков соответствует текущей конфигурации оборудования и программного обеспечения компании.

– Во-вторых, насколько актуальна информация о различных рисках? Информация об одних из них могла быть получена совсем недавно, в то время как оценка вероятности и важности других рисков может быть основана на достаточно старой информации.
– В-третьих, какие выводы нужно делать из имеющейся информации о рисках: какие действия нужно предпринять заранее, как идентифицировать факт срабатывания риска, как устранять последствия компьютерной атаки?

Программная система RiskPanel направлена на эффективное решение перечисленных задач. В отличие от конкурентных программных решений, она нацелена на постоянный мониторинг угроз безопасности корпоративной информационной системы. Анализ и учёт выявленных рисков, планирование действий по недопущению компьютерных атак и ликвидации их последствий происходит с учетом опыта уже произошедших в мире нарушений безопасности и понесенных потерь. Отличительной чертой системы является то обстоятельство, что связь между оценкой конкретных рисков и информацией о произошедших компьютерных атаках является для пользователя прозрачной и понятной.

Анализ рисков в системе RiskPanel заключается в том, что программный комплекс перманентно оценивает ситуацию информационной безопасности в компании, показывает администратору самые опасные риски нарушения безопасности, причины, из-за которых они проявляются, возможные методы их предотвращения. Все эти действия проводятся с учётом имеющейся и постоянно обновляющейся базы прецедентов компьютерных атак. Пользователю представляется список конкретных рисков, которые угрожают его компании и предлагаются возможные контрмеры, которые помогут закрыть уязвимости системы. Риски рассчитываются на основе знаний о прецедентах компьютерных атак и конфигурации информационной системы

компании. Конфигурация такой системы представляет собой оборудование, программное обеспечение, информационные потоки, персонал, финансовые потоки, компьютерные сети и др.

Программный комплекс RiskPanel имеет модульную структуру, позволяющую в дальнейшем подключать к нему новые модули. Например, к основным модулям была подключена система визуализации рисков, основанная на применении ДСМ-метода [20] и анализа формальных понятий [21]. В настоящее время программный комплекс имеет перечисленные далее три основных модуля.

1-й модуль. База знаний о прецедентах компьютерных атак и программная система постоянного оперативного пополнения базы данных. Задача этого модуля – осуществлять:

- пополнение информации по компьютерному терроризму и информационной безопасности;
- оперативное реагирование на появление новых видов компьютерных атак;
- предоставление интерфейса для ручной правки и внесения новой информации по компьютерной безопасности.

Данный модуль реализован на платформе OntoBox [22]. Эта платформа содержит систему хранения и обработки знаний, основанную на онтологиях. В основе OntoBox лежит идея использования «интеллектуальных» средств математической логики для решения задач построения информационных ресурсов. Система OntoBox позволяет применять логику описаний (Description Logic) [23] для представления данных. Это даёт возможность осуществлять логический вывод с целью получения новых знаний, исходя из имеющихся данных о прецедентах компьютерных атак. Информация о прецедентах компьютерных атак постоянно пополняется из Интернет и

других источников, обеспечивая, тем самым, актуальный анализ ситуации. Пополнение происходит в полуавтоматическом режиме.

2-й модуль. Программная система оценки рисков компьютерной атаки и уязвимостей корпоративной информационной системы. Задача этого модуля – осуществлять:

- риск-менеджмент безопасности корпоративной информационной системы;
- превентивные меры по предотвращению деструктивных воздействий, способных нанести ущерб компьютерным системам и сетям;
- пресечение компьютерной атаке на начальном этапе её реализации;
- оперативное устранение последствий компьютерной атаки и минимизация причинённого ущерба.

3-й модуль. Точная настройка системы компьютерной безопасности RiskPanel на конкретную корпоративную информационную систему. Задачи этого модуля:

- создание профиля данной корпоративной информационной системы, включающего основные параметры оборудования и программного обеспечения;
- организация выбора из базы данных информации по компьютерной безопасности, актуальной именно для данной корпоративной информационной системы;
- пополнение базы данных, исходя из профиля данной корпоративной информационной системы.

Программная система RiskPanel позволяет администратору информационной безопасности проводить достаточно тонкий анализ прецедентов компьютерных атак, имеющихся в базе знаний. Благодаря тому, что система хранения и обработки знаний OntoBox основана на логике описаний

(Description Logic), возможна отработка (выяснение истинности) любых утверждений, выразимых в логике описаний, о прецедентах компьютерных атак, их связях с угрозами, уязвимостями системы информационной безопасности, симптомами начала компьютерной атаки, её последствиями, возможными контрмерами и др. Заметим, что класс утверждений, которые могут быть выражены в логике описаний, является достаточно широким: логика описаний служит одним из средств онтологического моделирования предметных областей. Например, логика описаний лежит в основе языка описания онтологий OWL, продвигаемого WWW-консорциумом в рамках проекта Semantic Web.

Система визуализации позволяет пользователю удобным для него способом отслеживать связи между прецедентами компьютерных атак, угрозами, уязвимостями, симптомами, последствиями и контрмерами. Более того, пользователь может оценить напрямую связи между уязвимостями и симптомами, уязвимостями и контрмерами или последствиями, симптомами и последствиями и т.д. – в любых сочетаниях.

5. Заключение

В работе рассмотрены современные подходы к оценке рисков реализации компьютерных атак, необходимость в которых возникает при обеспечении безопасности корпоративной информационной системы. Проведён анализ достоинств и недостатков существующих программных систем, предназначенных для оценки таких рисков. Одним из недостатков традиционно используемых систем оценки рисков является тот факт, что пользователю предоставляется только числовая информация по оценке рисков, но не показывается, каким образом и на основе каких данных эти числовые оценки рисков были получены. В работе предложен подход к анализу рисков, направленный на устранение этого недостатка. Данный

подход основан на анализе прецедентов реально произошедших компьютерных атак. Прецеденты компьютерных атак представляются в виде, явно доступном для пользователя. С каждым прецедентом связываются уязвимости системы информационной безопасности, вследствие которых этот прецедент может произойти, симптомы начала компьютерной атаки, её последствия, контрмеры и др.

Изложены математические основы предлагаемого подхода к анализу прецедентов компьютерных атак и оценки рисков информационной безопасности. Исследуется специальный класс алгебраических систем – прецедентные модели, являющиеся частным случаем булевозначных моделей с атомной (в частности, с конечной) булевой алгеброй. Для получения числовой информации по оценке рисков информационной безопасности производится фазификация булевозначных моделей: по прецедентной модели строится нечеткая модель, в которой каждому предложению сопоставлена вероятность его истинности.

Описана программная реализация подхода к оценке рисков информационной безопасности, основанного на анализе прецедентов компьютерных атак – программная система RiskPanel. Система RiskPanel позволяет администратору информационной безопасности: в явном виде работать с прецедентами компьютерных атак, осуществляя превентивные меры, направленные на их предотвращение и недопущение нанесения ущерба компьютерным системам и сетям; пересекать деструктивные воздействия на начальных этапах их реализации; оперативно устранять последствия таких воздействий для минимизации ущерба, причинённого компании.

Литература

1. Васенин В.А. Информационная безопасность и компьютерный терроризм // В сб. "Научные и методологические проблемы информационной безопасности" (под ред. В.П. Шерстюка), М.: МЦНМО, 2004 г.
2. Варфоломеев А.А. *Управление информационными рисками: Учеб. пособие.* // – М.: РУДН, 2008. – 158 с.
3. Петренко С.А., Симонов С.В. *Управление информационными рисками. Экономически оправданная информация*. // Компания АйТи; ДМК Пресс, 2005. – 384с.
4. Нестеров С.А. *Анализ и управление рисками в информационных системах на базе операционных систем Microsoft*. // Библиотека учебных курсов MSDN Academic Alliance. 2007.
5. Paulk M.C., Curtis B., Chrissis M.B., Weber C.V. *Capability Maturity Model for Software, version 1.1.* // CMU/SEI-93-TR-024, – Februaru, 1993.
6. http://www.pcorp.u-net.com/risk.htm -- Интернет портал компании C&A Systems Security Ltd, разработчика ПО «COBRA».
7. http://www.aexis.de/RA%20ToolPage.htm -- RA Software Tool, демонстрационная версия метода.
8. http://www.cramm.com/ -- Интернет портал компании-разработчика ПО «CRAMM».
9. http://www.riskwatch.com/ -- Интернет портал компании Risk Watch International, разработчика ПО «RiskWatch».
10. http://dsec.ru/ -- Интернет портал компании Digital Security, разработчика ПО «Digital Security Office 2006».
11. http://www.cert.org/octave/ -- Интернет портал компании CERT® Coordination Center, разработчика ПО «OCTAVE».

12. http ://cve .mitre .org /cve – Интернет портал, поддерживающий каталог уязвимостей CVE.

13. Пальчунов Д.Е. *Решение задач поиска информации на основе онтологий.* // Бизнес-информатика, т.1, 2008, с. 3-13.

14. Пальчунов Д.Е. *Поиск и извлечение знаний: порождение новых знаний на основе анализа текстов естественного языка.* // Философия науки. 2009. №4(43) . с. 70-90.

15. Pal'chunov D.E. *Virtual catalog: the ontology-based technology for information retrieval.* // Lecture Notes in Artificial Intelligence, 6581, Springer-Verlag Berlin Heidelberg, 2011, pp. 164-183.

16. Власов Д.Ю., Пальчунов Д.Е., Степанов П.А. *Автоматизация извлечения отношений между понятиями из текстов естественного языка.* // Вестник НГУ. Серия: Информационные технологии. 2010. Т. 8, вып. 3. с. 23-33.

17. Palchunov D.E., Yakhyaeva G.E. *Interval fuzzy algebraic systems*. // Proceedings of the Asian Logic Conference 2005. World Scientific Publishers. 2006, pp. 23-37

18. Пальчунов Д.Е., Яхъяева Г.Э. *Нечеткие алгебраические системы*. // Вестник НГУ. Серия: Математика, механика, информатика. 2010. Т.10, вып. 3. С. 75-92.

19. Promislow S.D. *Fundamentals of Actuarial Mathematics*. // John Wiley and Sons, 2011. 466 pp.

20. *ДСМ-метод автоматического порождения гипотез: Логические и эпистемологические основания*. // Сост. Аншаков О.М., Фабрикантова Е.Ф.; Под общ. Ред. Аншакова О.М. – М.: Книжный дом «ЛИБРОКОМ», 2009. – 432 с.

21. Ganter, Bernhard; Stumme, Gerd; Wille, Rudolf, eds. *Formal Concept Analysis: Foundations and Applications*. // Lecture Notes in Artificial Intelligence, no. 3626. Springer-Verlag, 2005. – 372 pp.

22. Малых А.А., Манцивода А.В., *Онтобокс: онтологии для объектов*. // Известия Иркутского государственного университета, Т. 2, № 2. 2009, с. 94-104.

23. *The Description Logic Handbook. //* by: Baader F. New York: Cambridge University Press, 2003. – 555 pp.

D.E. Palchunov, G.E. Yakhyaeva, A.A. Hamutskaya

SOFTWARE SYSTEM FOR INFORMATION RISK MANAGEMENT «RiskPanel»

Annotation: We consider the modern approaches to estimating risks to information security of corporate information system. The analysis of software systems intended for estimation of such risks is carried out. We present an approach to risk analysis based on construction of formal models of precedents of cyber attacks. Mathematical foundations of the presented approach are stated. Finally we describe software system RiskPanel which is an implementation of our approach.

Keywords: information security, cyber attack, risk management, corporate information system, fuzzy model