УДК 004.056 **DOI:10.30837/rt.2021.3.206.08**

В.В. ВИЛИГУРА, В.И. ЕСИН, д-р техн. наук

МОДЕЛЬ ЗАЩИТЫ БАЗЫ ДАННЫХ НА ОСНОВЕ СИСТЕМЫ БЕЗОПАСНОСТИ С ПОЛНЫМ ПЕРЕКРЫТИЕМ

Введение

Безопасность (защищенность) является одной из важнейших характеристик качества [1] информационных систем (ИС) в целом и баз данных (БД) как их основной составляющей, в частности. Наличие системы защиты информации как комплекса программных, технических, криптографических, организационных и иных методов, средств и мероприятий, обеспечивающих целостность, конфиденциальность, аутентичность и доступность информации в условиях воздействия на нее угроз естественного или искусственного характера, является неотъемлемой чертой любой современной ИС, БД. При этом высокая степень безопасности данных должна быть обеспечена без снижения функциональности ИС, БД и практически без усложнения работы пользователя в системе [2]. Вместе с тем, чтобы можно было проверить выводы о степени обеспечения безопасности, ее необходимо каким-либо образом измерить. При этом известно [3], что обеспечить безопасность информационной системы легче, если есть четкая модель того, что нужно защищать и кому и что разрешено делать.

Поэтому, после анализа и обобщения различных подходов и достижений в области оценки безопасности информационных систем в целом и баз данных в частности было принято решение в качестве модели защиты БД, и оценки ее безопасности использовать модель Клементса – Хоффмана [4, 5], опирающуюся на теорию графов, нечетких множеств, вероятностей, и традиционно считающуюся основой формального описания систем защиты.

Формализация задачи обеспечения безопасности баз данных

Основным положением *модели системы безопасности с полным перекрытием* (модель Клементса – Хоффмана) является тезис о том, что система, спроектированная на ее основе, должна иметь, по крайней мере, одну меру (механизм, метод, средство) для обеспечения безопасности на каждом возможном пути проникновения в систему. В модели рассматривается взаимодействие «области угроз», «защищаемой области» и «системы защиты». Считается, что несанкционированный доступ (как любой доступ, нарушающий заявленную политику безопасности [6]) к каждому из набора объектов O защищаемой области сопряжен с некоторой величиной ущерба, который может быть определен количественно (в противном случае его полагают равным некоторой условной величине). При этом количественная категория ущерба может быть выражена в стоимостном эквиваленте (сумма финансовых потерь), либо в терминах, связанных с целевой функцией системы (например, времени, необходимом для восстановления функциональных возможностей ИС в целом, и БД в частности, после злоумышленного воздействия) [7].

Для описания системы безопасности с полным перекрытием применительно к базам данным введем следующие обозначения:

– $T=\{t_i\}$, $i=1..I$ – множество угроз безопасности БД. Для формирования набора угроз, направленных на нарушение безопасности, по возможности, определяются все потенциальные злоумышленные действия по отношению ко всем объектам безопасности;

– $O=\{o_j\}$, $j=1..J$ – множество защищаемых объектов БД;

– $W=\{w_k\}$, $k=1..K$ – множество мер обеспечения безопасности (в том числе, методов, средств, механизмов, обеспечивающих реализацию политик безопасности, формальным представлением которых являются модели безопасности, методов и примитивов для защиты информации БД, основанных на криптографии).

Элементы всех перечисленных множеств находятся между собой в определенных отношениях, причем связь между угрозами и объектами не является связью «один к одному». Угроза $t_i \in T$ может распространяться на любое число объектов O, а объект $o_j \in O$ может быть уязвим со стороны более чем одной угрозы T. Для лучшего понимания систему защиты в рамках данной формализации целесообразно представить двухдольным графом (рис. 1), в котором множество отношений «угроза – объект» представляется в виде дуг (t_i, o_j), существующих только тогда, когда t_i является угрозой, направленной на нарушение безопасности объекта $o_j \in O$.

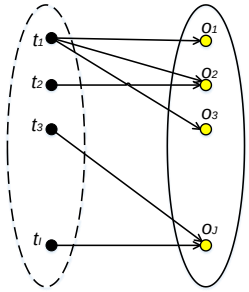

Рис. 1. Представление отношения «объект – угроза»

Защита обеспечивается путем перекрытия всех возможных дуг графа, за счет создания соответствующего барьера (средства обеспечения безопасности $w_k \in W$) на каждом пути. В результате двухдольный граф преобразуется в трехдольный (рис. 2).

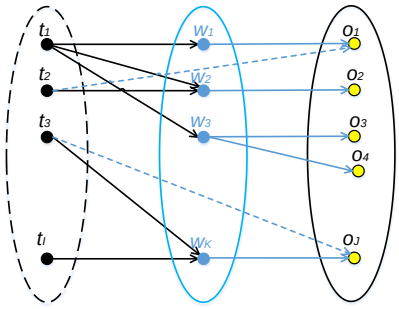

Рис. 2. Представление отношений между угрозами, средствами обеспечения безопасности и объектами

В защищенной системе все дуги модели представляются в виде (t_i, w_k) и (w_k, o_j). Любая дуга (t_i, o_j) определяет незащищенный объект (дуги (t_2, o_1) и (t_3, o_J) на рис. 2). При этом следует заметить, что одно и то же средство обеспечения безопасности может перекрывать более одной угрозы и/или защищать более одного объекта.

В дальнейшем для построения модели воспользуемся так называемой базовой системой обеспечения безопасности Клементса, описанной в работах [4, 5], в виде 5-мерного кортежа (пятерки): $S = \{O, T, W, V, B\}$, которая предполагает включение набора уязвимостей V (представляющих собой пути реализации угроз T в отношении объектов O), определяемого подмножеством декартова произведения $V = T \times O$ (набором упорядоченных пар $v_r = (t_i, o_j)$, $r = 1..R$) и набора барьеров (представляющих собой точки, в которых требуется осуществлять защиту) B, определяемого подмножеством декартова произведения $B = V \times W = T \times O \times W = \{b_l = (t_i, o_j, w_k),\ l = 1..\Lambda\}$ как отображение $T \times O \times W$ на набор упорядоченных троек $b_l = (t_i, o_j, w_k)$.

Для данной модели условие полного перекрытия можно записать в следующем виде: $\forall (v_r = (t_i, o_j)) \in V$, $\exists (b_l = (t_i, o_j, w_k)) \in B$. Это условие означает, что для каждого пути реали-

зации угроз T в отношении объектов O средством безопасности $w_k \in W$ создается барьер $b_l \in B$, устраняющий эту угрозу для конкретного объекта.

В идеале каждый механизм защиты (меры безопасности) должен исключать соответствующий путь реализации угрозы. На практике эти механизмы обеспечивают лишь некоторую степень сопротивляемости угрозам безопасности (например, пароли имеют конечную длину; шифры имеют различную криптографическую стойкость; различная частота точек синхронизации между базой данных и журналом транзакций приводит к всевозможным, иногда неприемлемым, временам восстановления при сбоях, отказах; зависимость защищенности от актуальности и своевременности устанавливаемых параметров конфигурации и т. д.).

Показатель защищенности базы данных

Чтобы иметь некоторую количественную оценку уровня защищенности объектов, авторы модели системы безопасности с полным перекрытием [4, 5] считают, что можно измерить степень обеспечения безопасности системы. В качестве подходящей структуры для выражения таких мер они предлагают лингвистическую переменную, которая принимает значения в виде слов, а не чисел. Для этого они переопределяют барьеры безопасности B, каждый из которых ($b_l \in B$) представляют в виде составной лингвистической переменной, компонентами которой являются лингвистические переменные: P_l – вероятность возникновения угрозы; L_l – величина ущерба при успешной реализации угрозы в отношении защищаемого объекта; R_l – степень сопротивляемости средства защиты w_k, характеризующаяся вероятностью его преодоления. При этом отмечается, что эти компоненты оцениваются в контексте специфического барьера ($b_l = (t_i, o_j, w_k)$), который они формируют (индексы у P_l, L_l, R_l такие же, как индекс барьера, а не такие, как у компонентов барьера $b_l = (t_i, o_j, w_k)$ в базовой системе защиты – угрозы, объекты и средства защиты). Авторы поясняют, что значение сопротивляемости определяет степень повышения или снижения общей безопасности системы, а неформальная комбинация вероятности и величины потерь дает важность (вес) барьера в сводном рейтинге (оценке), и в целом эти значения определяют вклад барьера в общую безопасность системы. При этом они ничего не говорят о конкретных способах их получения (оценивания), а также о существовании, виде и использовании интегрального показателя, позволяющего оценивать защищенность объектов и системы в целом. Поэтому, после анализа различных подходов, изложенные в релевантных источниках [8 – 10], в качестве такого показателя был выбран остаточный риск Rr, связанный с возможностью реализации угрозы $t_i \in T$ в отношении объекта БД $o_j \in O$ при использовании средства обеспечения безопасности $w_k \in W$. Величину остаточного риска, характеризующего стойкость (прочность) барьера $b_l \in B$, можно определить следующим образом [8, 9]:

$$Rr_l = P_l L_l (1 - R_l). \tag{1}$$

Остаточный риск, по сути, является мерой незащищенности актива. Тогда величину защищенности БД можно определить путем вычисления обратной величины суммарного остаточного риска подобно [8, 9]:

$$S = \sum_{\forall b_l \in B} \frac{1}{P_l L_l (1 - R_l)}, \tag{2}$$

где $P_l, L_l \in (0,1)$, $R_l \in [0,1)$.

При отсутствии в системе барьеров b_l, перекрывающих определенные пути реализации угроз в отношении объектов, степень сопротивляемости механизма защиты R_l принимается равной нулю. С формальной стороны это можно представить путем ввода так называемого средства защиты с нулевой степенью обеспечения безопасности (w_o), добавляемого ко множеству W [4, 5]. Каждому незащищенному объекту приписывается такое средство. Таким образом, для $\forall(t_i, o_j) \in V$, для которого $(\forall k \in K)\ (t_i, o_j, w_k) \notin B$, к B добавляется барьер (t_i, o_j, w_o).

Особенности предлагаемой модели защиты БД

Следует отметить еще одну особенность рассматриваемой модели. Авторы [5], вводя понятие уязвимости (англ. vulnerability), формально представляют его как отображение $T \times O$ на набор упорядоченных пар $v_r = (t_i, o_j)$, а не отдельно объективно существующую категорию уязвимости как слабого места актива или средства управления, которое может быть использовано одной или более угрозой [11]. Угрозы существуют отдельно от слабых мест актива. Уязвимость сама по себе не наносит ущерба, это только условие или набор условий, позволяющих угрозе причинить ущерб активам. При реализации угрозы может использоваться одна или более уязвимостей актива [12]. При этом один тип уязвимости может привести к множеству угроз безопасности различной направленности. Поэтому угрозы и уязвимости целесообразно рассматривать в комплексе. Только вместе они могут стать причиной нежелательного инцидента, который может причинить вред системе (активам). И в этом случае необходимо четко определить угрозы, уязвимости и взаимосвязь между ними.

В связи с этим расширим представленную выше модель с полным перекрытием до 6-мерного кортежа (шестерки) за счет включения множества уязвимостей (слабых мест) объектов (Γ):

$$S' = \{O, T, \Gamma, W, V, B\}. \tag{3}$$

Тогда после соответствующего уточнения модели под набором V будем понимать множество упорядоченных троек $v_r = (t_i, \gamma_\psi, o_j)$, $\psi = 1..\Psi$, где $\gamma_\psi \in \Gamma$ – уязвимость (как некоторый ее тип), используемая угрозой $t_i \in T$, направленной на нарушение безопасности объекта $o_j \in O$. Набор барьеров будет соответственно определяться как: $B = V \times W = T \times \Gamma \times O \times W = \{b_l = (t_i, \gamma_\psi, o_j, w_k),\ l = 1..L\}$. А условие обеспечения полной защищенности для данной модели примет следующий вид: $\forall(v_r)$, $\exists(b_l = (t_i, \gamma_\psi, o_j, w_k)) \in B$. Это условие означает, что для каждой тройки (t_i, γ_ψ, o_j) из множества V создается барьер $b_l \in B$, что делает невозможным реализацию нежелательного инцидента (реализацию угрозы $t_i \in T$, использующей уязвимость $\gamma_\psi \in \Gamma$) в отношении объекта защиты $o_j \in O$.

Средство защиты с нулевой степенью обеспечения безопасности (w_o), добавляемое к множеству W и приписываемое к незащищенному объекту, формально можно выразить следующим образом: для $\forall(t_i, \gamma_\psi, o_j) \in V$, для которого $(\forall k \in K)\ (t_i, \gamma_\psi, o_j, w_k) \notin B$, к B добавляется барьер $(t_i, \gamma_\psi, o_j, w_o)$.

Соответственно в выражениях (1), (2) под вероятностью P_l будет пониматься вероятность нежелательного инцидента (реализации угрозы) как произведение вероятности возникновения угрозы P_{t_i} на вероятность использования (удачного) уязвимости P_{γ_ψ}: $P_l = P_{t_i} \cdot P_{\gamma_\psi}$ [10, 13]. То есть в данном случае используется так называемая двухфакторная

модель оценки вероятности [14], выделяющая два компонента (фактора), один из которых отображает мотивационную составляющую возникновения угрозы, а второй учитывает существующие уязвимости. Величину ущерба L_l в отношении защищаемого объекта следует рассматривать с позиции успешной реализации угрозы t_i, использующей уязвимость γ_ψ.

Исходя из сказанного, для описания системы безопасности с полным перекрытием применительно к базам данным конкретизируем элементы множеств защищаемых объектов БД, угроз и уязвимостей, характерных для БД, мер (средств контроля) обеспечения безопасности. А именно, определим объекты защиты БД $o_j \in O$ с характерным для них списком угроз $t_i \in T$ и уязвимостей $\gamma_\psi \in \Gamma$, благодаря которым становится возможной реализация соответствующей угрозы, а также идентифицируем реализованные средства/меры обеспечения безопасности $w_k \in W$.

Учитывая, что системы БД являются информационными продуктами с двойственной природой – двумя компонентами (активами) в виде программных средств СУБД, независимых от сферы их применения, структуры, смыслового содержания накапливаемых и обрабатываемых данных и собственно хранимых данных, возможность вредоносного воздействия на эти активы, целесообразным является обеспечение безопасности их обоих. Для реляционных БД, как получивших наибольшее распространение (этот тезис подтверждают результаты DB-Engines и PYPL рейтингов [15, 16], а также отчеты экспертов всемирно известной компании Gartner, Inc. [17, 18]), с учетом возможности различной степени детализации этих компонент можно выделить следующие объекты защиты [19, 20]:

– базу данных в целом – o_1;

– таблицы – o_2;

– представления (views) – o_3;

– картежи (строки) таблиц – o_4;

– отдельные поля (значения атрибутов) строк – o_5;

– триггеры – o_6;

– постоянно хранимые модули – o_7 и некоторые другие.

Основными наиболее крупными и важными угрозами (типами угроз) безопасности баз данных, носителями которых являются различные источники угроз (в большей мере нас будут интересовать антропогенные – люди или группы лиц, в результате действий либо бездействия которых произошло нарушение безопасности рассматриваемой системы [21], в том числе с возможными сценариями действий злоумышленников (на примере СУБД Oracle), представленными на рис. 3), согласно [19, 22 – 27] являются:

– чрезмерные и неиспользуемые привилегии. Для определенности обозначим этот тип угрозы как t_1;

– злоупотребление законными привилегиями – t_2;

– инъекции ввода – t_3;

– вредоносное программное обеспечение – t_4;

– недостаточность мер по аудиту данных (слабые аудиторские следы) – t_5;

– незащищенность носителей (резервных копий) информации – t_6;

– эксплуатация уязвимых, неверно сконфигурированных баз данных – t_7;

– неуправляемые конфиденциальные данные – t_8;

– логический вывод – t_9;

– отказ в обслуживании – t_{10};

– недостаток знания и опыта в вопросах информационной безопасности – t_{11} и некоторые другие.

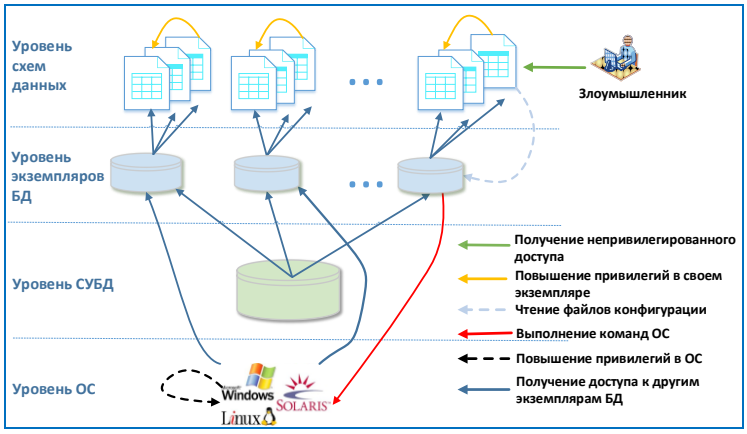

Рис. 3. Схема возможных действий злоумышленника

На основе анализа существующих таксономий уязвимостей, имеющих отношение к конкретному экземпляру продукта или системы (а не к основным недостаткам), которые могут быть непосредственно использованы злоумышленником для реализации угроз безопасности [28], общих слабых мест (англ. weakness) программного и аппаратного обеспечения, которые могут привести к возникновению уязвимостей [29, 30], а также некоторых других классификаций уязвимостей и недостатков безопасности активов [21, 31, 32] был определен перечень основных общих слабых мест (недостатков) как некоторых типов уязвимостей. За основу взята спецификация из Common Weakness Enumeration (CWE), точнее, классификация абстрактного представления Концепции исследования (Research Concepts) CWE [33], используемая академическими исследователями, аналитиками уязвимостей, поставщиками средств оценки. С учетом специфики рассматриваемых аспектов, обусловленных характерными особенностями обеспечения безопасности, присущими базам данных и СУБД (не принимая в расчет возможности реализации угроз посредством уязвимостей, связанных с недостатками в программном обеспечении, архитектуре и конфигурировании сетей и операционных систем), в их число вошли основные слабые места достаточно высокого уровня абстракции:

1) *неправильное управление привилегиями*: неправильное назначение привилегий, повышение (эскалация) привилегий, выполнение операций с излишними привилегиями;

2) *неправильная авторизация*: неправильное назначение разрешений для критического ресурса, отсутствует авторизация, некорректная авторизация, раскрытие конфиденциальной информации через метаданные, раскрытие конфиденциальной информации посредством запросов данных. Не выполняется или неправильно выполняется проверка авторизации, когда субъект пытается получить доступ к ресурсу или выполнить некоторое действие;

3) *неправильная аутентификация*: слабый пароль, устаревший пароль, обход аутентификации, неправильная реализация алгоритма аутентификации, несоответствующий срок действия сеанса и т. д.;

4) *неконтролируемое потребление ресурсов*: надлежащим образом не контролируется распределение ограниченного ресурса, тем самым позволяя субъекту влиять на количество потребляемых ресурсов, что в конечном итоге приводит к их исчерпанию;

5) *хранение конфиденциальной информации в открытом виде*;

6) *недостаточная стойкость шифрования*;

7) *неправильная очистка конфиденциальных данных с выведенного из эксплуатации устройства*: очистка может отсутствовать, быть недостаточной или некорректной;

8) *использование взломанного или опасного криптографического алгоритма*: использование нестандартного, с недоказанной стойкостью криптографического примитива;

9) *использование недостаточно случайных значений*;

10) *недостаточная проверка подлинности данных*: загрузка кода без проверки целостности, неправильная проверка (отсутствие проверки) значения контрольной суммы, неправильная проверка (отсутствие проверки) криптографической подписи;

11) *неправильная проверка ввода*: неправильная проверка синтаксической правильности входных данных, неправильная проверка указанного типа входных данных, неправильная проверка согласованности входных данных, неправильная проверка небезопасной эквивалентности входных данных. Входные данные или не проверяются, или проверяются неправильно – без гарантии того, что их использование не приведет в дальнейшем к неправильной и небезопасной обработки данных;

12) *использование запрещенного кода*: используются функции, библиотеки или сторонние компоненты, которые были явно запрещены разработчиком или заказчиком;

13) *встроенный вредоносный код*;

14) *нарушение принципов безопасного проектирования*: ненужная сложность в механизме защиты (используется более сложный механизм, чем необходимо); опора на единственный фактор при принятии решения о безопасности; недостаточно разделяются функциональность или процессы, требующие различных уровней привилегий, прав или разрешений; не предусмотрена проверка доступа к защищаемому объекту, выполняемая каждый раз при обращении субъекта к этому объекту; недостаточная психологическая приемлемость (сложность и неудобство использования механизма защиты зачастую побуждает пользователей незлоумышленников отключать или обходить его случайно или намеренно); опора на безопасность через неизвестность (используется механизм защиты, сила которого в значительной степени зависит от его неизвестности); несовершенство механизма поддержки целостности данных;

15) *некорректное предоставление указанной функциональности*: код не работает в соответствии с опубликованными спецификациями, что может привести к неправильному использованию;

16) *скрытая функциональность*: имеется функциональность, которая не задокументирована, не являются частью спецификации и недоступна через интерфейс или последовательность команд. Скрытая функциональность может принимать разные формы, в том числе, например, такие, как преднамеренно вредоносный код;

17) *неполная документация*: нет описаний всех соответствующих элементов продукта, таких как его использование, структура, интерфейсы, проектирование, реализация, конфигурация, эксплуатация и т. д., что усложняет обслуживание, косвенно влияя на безопасность из-за недостаточной осведомленности, затрудняя поиск и/или исправление уязвимостей или отнимая много времени, что также может упростить внедрение уязвимостей;

18) *изъян конфигурации*: несоблюдение требований безопасности при инсталляции и конфигурации БД (установлены административные, вспомогательные, учебные учетные записи, прописываемые в БД по умолчанию без надлежащего их анализа и смены паролей по умолчанию, не установлены ограничения на длину и сложность паролей, не заблокированы неиспользуемые учетные записи, не установлены критические обновления, ненадлежащим образом настроена система аудита событий и т. д.).

Для определенности обозначим их соответственно как $\gamma_1,...,\gamma_{18}$.

После идентификации угроз и уязвимостей, а также оценки возможности их связывания необходимо определить вероятности нежелательного инцидента (реализации угрозы) для соответствующих пар «угроза-уязвимость» (t_i, γ_ψ), где $i=\overline{1,11};\ \psi=\overline{1,18}$ как произведение вероятности возникновения соответствующей угрозы P_{t_i} на вероятность соответствующей уязвимости P_{γ_ψ} : $P_l = P_{t_i} \cdot P_{\gamma_\psi}$.

Метод оценивания основных компонент барьеров безопасности и защищенности базы данных в целом

Нетрудно видеть, что при известных значениях вероятности нежелательного инцидента (реализации угрозы) P_l, величины ущерба L_l (при удачном осуществлении угрозы в отношении защищаемого объекта), степени сопротивляемости соответствующего средства защиты R_l можно оценить защищенность БД, воспользовавшись выражением (2).

Однако получение точных значений P_{t_i}, P_{γ_ψ}, L_l, R_l непростая задача. Зачастую на практике это не представляется возможным [12]. К тому же, перефразируя Заде [34], по мере увеличения сложности системы аналитическая точность уменьшается [5]. Поэтому, как правило, в таких случаях целесообразно прибегнуть к числовым оценкам в некотором диапазоне величин, тем более, что каждому количественному диапазону можно сопоставить определенную качественную шкалу, с которой при определенных потребностях работать существенно проще. Подходящей структурой для выражения таких величин, как отмечалось выше, может служить лингвистическая переменная. По этим причинам, в первую очередь, в соответствии с введенными изменениями модели переопределим барьеры безопасности B, каждый из которых ($b_l \in B$) представим в виде составной лингвистической переменной, компонентами которой являются лингвистические переменные: вероятность возникновения угрозы P_t, вероятность использования уязвимости P_γ, величина ущерба L при удачном осуществлении угрозы в отношении защищаемого объекта, степень сопротивляемости средства защиты R, характеризующаяся вероятностью его преодоления. При этом замечаем, что данные компоненты оцениваются в контексте специфического барьера, который они формируют. (Индексы у $P_l = f(P_{t_i}, P_{\gamma_\psi}), L_l, R_l$ такие же, как индекс барьера, а не такие, как у компонентов барьера $b_l = (t_i, \gamma_\psi, o_j, w_k)$ – угрозы, уязвимости, объекта и средства защиты в базовой системе защиты.)

Формализацию соответствующих компонент начнем с вероятности возникновения угрозы P_t, которая может быть представлена в виде лингвистической переменной:

$$\langle name, T, X, G, M \rangle, \tag{4}$$

где $name$ – наименование лингвистической переменной (в нашем случае – это вероятность возникновения угрозы P_t); T – множество значений лингвистической переменной (терм-множество), представляющих собой наименования нечетких переменных (α_ε, где $\varepsilon = 1, 2, ...$ ($\varepsilon \in \mathbb{N}^*_{<n}$), n – максимальное число нечетких переменных), областью определения каждой из которых является множество X – универсальное множество или универсум (в рассматриваемом случае это числовые значения вероятности возникновения угрозы); G – некоторая синтаксическая процедура, позволяющая оперировать элементами терм-множества T, в частности – генерировать новые термы (значения); M – семантическая процедура, позволяющая превратить каждое новое значение лингвистической переменной, получаемое с помощью процедуры G, в нечеткую переменную, то есть сформировать соответствующее нечеткое множество. В рассматриваемом случае можно ограничиться предположением о тривиальном характере G и M, то есть никаких логических связок и модификаторов использоваться не будет.

Вероятность возникновения той или иной угрозы информации определяется экспертным путем на основании показателя, характеризующего, насколько вероятно возникновение угрозы безопасности в рассматриваемой системе с учетом особенностей ее структуры и функционирования. На практике для вычисления риска зачастую используется не математическая вероятность угрозы, а примерная частота ее реализации за определенный период времени.

Чтобы не было путаницы, вместо математического термина *probability* в стандартах намеренно используется понятие *likelihood*, которое также переводится как «вероятность». При этом эксперты не определяют функцию правдоподобия в статистическом смысле. Вместо этого они на основе имеющихся данных, опыта и экспертных суждений определяют балл (рейтинг – англ. score) вероятности [35].

Анализ различных авторитетных источников по проблемам управления информационными рисками [12, 35 – 39] показал, что для оценки P_t достаточно ввести три вербальные градации с соответствующими приблизительными количественными оценками, без которых любая качественная шкала лишается смысла:

– низкая вероятность (Н). Возникновение данной угрозы маловероятно. Не существует инцидентов, статистики, мотивов, которые указывали бы на то, что это может произойти. Ожидаемая частота угрозы не превышает одного раза в пять лет;

– средняя вероятность (С). Существуют предпосылки к появлению угрозы (зафиксированы случаи, в прошлом происходили инциденты), существует статистика или имеется другая информация, указывающая на возможность возникновения данной угрозы, у злоумышленника есть мотивация для реализации соответствующих действий. Ожидаемая частота появления данной угрозы – примерно один раз в год;

– высокая вероятность (В). Имеются объективные предпосылки для возникновения угрозы. Существуют инциденты, статистика или другая информация, указывающая на то, что угроза, скорее всего, осуществится, у злоумышленника есть мотивы для реализации соответствующих действий. Ожидаемая частота появления угрозы – в среднем один раз в четыре месяца или чаще.

Такой трехуровневой шкалы обычно достаточно для первоначальной высокоуровневой оценки. В дальнейшем ее можно расширить, добавив еще несколько промежуточных уровней. При этом следует отметить, что оценки ожидаемой частоты возникновения угрозы от уровня к уровню по качественной шкале различаются в разы, поэтому маловероятно, чтобы компетентные эксперты сильно ошибались бы в своих оценках.

С другой стороны, частотную оценку имеющейся величины можно преобразовать в числовой эквивалент вероятности возникновения угрозы, соответствующий некоторому диапазону значений. Под термином «вероятность» в данном случае понимается так называемая субъективная вероятность – мера уверенности некоторого человека или группы людей (агентов) в том, что данное событие в действительности будет иметь место [37, 40].

Исходя из обобщения проанализированных источников [37, 38, 41], будем полагать, что в числовом эквиваленте вероятность возникновения такой угрозы на соответствующем уровне может находиться в соответствующем ей диапазоне:

– для уровня Н – $P_t = [0, 0.2]$;

– уровня С – $P_t = [0.2, 0.6]$;

– уровня В – $P_t = [0.6, 1]$.

Тогда, воспользовавшись применяемыми при оценке рисков информационной безопасности известными качественными шкалами [12, 35 – 37, 39], в частности трехуровневой качественной шкалой, определим наименования нечетких переменных – множество значений терм-множества T: T ={«низкая вероятность», «средняя вероятность», «высокая вероятность»}={«Н», «С», «В»}, то есть α_1=«Н», α_2 = «С», α_3=«В».

Как известно, когда речь идет о нечеткой переменной α, всегда имеется в виду некоторое нечеткое множество $A = \{\mu_A(x) / x\}$, которое определяет ее возможные значения, где $\mu_A(x)$ – *функция принадлежности* ($\mu_A(x) \in [0,1]$; $\mu_A(x): X \to [0,1]$), которая указывает степень принадлежности элемента x нечеткому множеству A.

Наибольшее распространение при построении функций принадлежности нечетких множеств получили прямые и косвенные методы [42, 43]. Ввиду того, что $x \in X$ могут быть из-

мерены в количественной шкале, воспользуемся прямым методом, когда эксперт либо группа экспертов задают для каждого $x \in X$ значение функции принадлежности $\mu_A(x)$. При этом, как отмечается в работе [42], теория нечетких множеств при использовании прямых методов построения функции принадлежности не требует абсолютно точного ее задания. Очень часто бывает достаточно зафиксировать лишь наиболее характерные значения и вид (тип) функции $\mu_A(x)$. Сама же функция принадлежности может быть определена [44]: графически (график, диаграмма); аналитически (формулы); в виде таблицы, суммы или интеграла, вектора степеней принадлежности. Как показывает опыт, удобно использовать те функции принадлежности, которые допускают аналитическое представление в виде некоторой простой математической функции [42].

На основании анализа основных функций принадлежности, использующихся для представления таких свойств нечетких множеств, которые характеризуются неопределенностью типов «небольшое значение», «незначительная величина»; «расположен в интервале», «приблизительно равно»; «большое значение», «значительная величина», для рассматриваемых нечетких переменных «Н», «С», «В» были выбраны трапециевидная, линейная Z- и линейная S-образные функции. Каждая из этих функций может быть представлена так:

– линейная Z-образная функция принадлежности нечеткого множества $A_{\text{Н}} = \{\mu_{\text{Н}}(x)/x\}$, соответствующего нечеткой переменной «Н» для лингвистической переменной – вероятность возникновения угрозы P_t:

$$\mu_{\text{Н}}(x;a,b) = \begin{cases} 1, & x \le a, \\ \dfrac{b-x}{b-a}, & a < x < b, \\ 0, & b \le x, \end{cases} \tag{5}$$

где a, b – упорядоченные отношением $a \le b$, числовые параметры;

– трапециевидная функция принадлежности нечеткого множества $A_{\text{С}} = \{\mu_{\text{С}}(x)/x\}$, соответствующего нечеткой переменной «С» для лингвистической переменной P_t:

$$\mu_{\text{С}}(x;a,b,c,d) = \begin{cases} 0, & x \le a, \\ \dfrac{x-a}{b-a}, & a \le x \le b, \\ 1, & b \le x \le c, \\ \dfrac{d-x}{d-c}, & c \le x \le d, \\ 0, & d \le x, \end{cases} \tag{6}$$

где a, b, c, d – упорядоченные отношением: $a \le b \le c \le d$, числовые параметры;

– линейная S-образная функция принадлежности нечеткого множества $A_{\text{В}} = \{\mu_{\text{В}}(x)/x\}$, соответствующего нечеткой переменной «В» для лингвистической переменной P_t:

$$\mu_B(x;c,d) = \begin{cases} 0, & x \le c, \\ \dfrac{x-c}{d-c}, & c < x < d, \\ 1, & d \le x, \end{cases} \tag{7}$$

где c, d – числовые параметры ($c \le d$).

На рис. 4 представлены все три графика функций принадлежности нечетких переменных, используемых для задания лингвистической переменной – вероятность возникновения угрозы P_t.

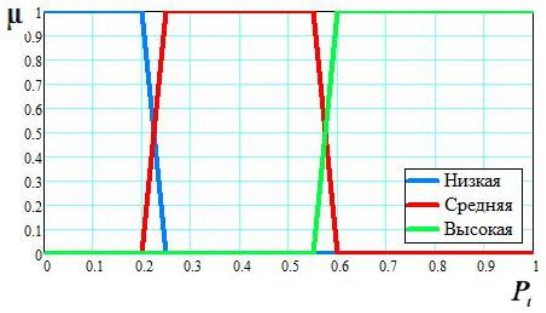

Рис. 4. Графики функции принадлежности нечетких множеств $A_{\text{Н}}$, $A_{\text{С}}$, $A_{\text{В}}$

Эксперт на основании априорных знаний присваивает лингвистические значения, представляющие собой наименования нечетких переменных, для каждой вероятности возникновения угрозы P_{t_i} как компоненты соответствующего специфического барьера b_l. В данном случае эти значения могут представляться вербально как: «низкая вероятность», «средняя вероятность», «высокая вероятность» (или «Н», «С», «В»). Поскольку с каждым таким значением связывается соответствующая функция принадлежности с соответствующими приблизительными количественными оценками, то, в принципе, для каждой угрозы $t_i \in T$ можно определить с ограниченной степенью точности численное значение этой вероятности P_{t_i}, например, как *модальное значение нечеткого множества*. Если ядро нечеткого множества содержит более одного элемента, то для такого множества модальное значение определяется как среднее значение элементов ядра. *Ядро нечеткого множества* A представляет собой четкое подмножество области определения X, содержащее все элементы, принадлежащие множеству A со степенью, равной 1 [44].

Далее, воспользовавшись изложенным подходом, представим в виде соответствующей лингвистической переменной вероятность использования уязвимости – P_γ (вероятность того, что в случае реализации угрозы в отношении актива эта угроза будет реализована успешно с использованием данной уязвимости). Уязвимости так же, как и угрозы, могут быть оценены по трехуровневой качественной шкале. Для оценки P_γ введем три вербальные градации с соответствующими приблизительными количественными оценками:

– высокая (В). Уязвимость легко использовать, и существует слабая защита или защита вообще отсутствует. Вероятность использования уязвимости (вероятность успешной реализации угрозы за счет данной уязвимости) находится в диапазоне [0.7, 1];

– средняя (С). Уязвимость может быть использована, но существует определенная защита. Вероятность использования уязвимости находится в диапазоне [0.3, 0.7];

– низкая (Н). Уязвимость сложно использовать, и существует хорошая защита. Вероятность использования уязвимости находится в диапазоне [0, 0.3].

Так же, как и с угрозами, для первоначальной высокоуровневой оценки уязвимостей вполне может хватить такой трехуровневой шкалы. В дальнейшем для более детальной оценки ее можно расширить.

Воспользовавшись введенными обозначениями, определим наименования нечетких переменных (β_ε, где $\varepsilon \in \square^*_{<n}$) – множество значений терм-множества T_γ лингвистической переменной P_γ: T_γ={«высокая уязвимость», «средняя уязвимость», «низкая уязвимость»}={«В», «С», «Н»}, то есть β_1=«В», β_2= «С», β_3=«Н». Областью определения каждой из нечетких переменных является множество числовых ($X \in [0,1]$) значений вероятности использования уязвимости. В рассматриваемом случае тоже можно ограничиться предположением о тривиальном характере G_γ и M_γ (без логических связок и модификаторов).

На основании анализа основных функций принадлежности, подобно приведенному выше, для рассматриваемых нечетких переменных β_1=«В», β_2= «С», β_3=«Н» были выбраны трапециевидная, линейная Z- и линейная S-образные функции. Каждая из этих функций может быть представлена как:

– линейная Z-образная функция принадлежности нечеткого множества $A_{\text{Н}}^{v} = \{\mu_{\text{Н}}^{v}(x)/x\}$, соответствующего нечеткой переменной «Н» для лингвистической переменной P_γ:

$$\mu_{\text{Н}}^{v}(x;a,b) = \begin{cases} 1, & x \le a, \\ \dfrac{b-x}{b-a}, & a < x < b, \\ 0, & b \le x; \end{cases} \tag{8}$$

– трапециевидная функция принадлежности нечеткого множества $A_{\text{С}}^{v} = \{\mu_{\text{С}}^{v}(x)/x\}$, соответствующего нечеткой переменной «С» для лингвистической переменной P_γ:

$$\mu_{\text{С}}^{v}(x;a,b,c,d) = \begin{cases} 0, & x \le a, \\ \dfrac{x-a}{b-a}, & a \le x \le b, \\ 1, & b \le x \le c, \\ \dfrac{d-x}{d-c}, & c \le x \le d, \\ 0, & d \le x; \end{cases} \tag{9}$$

– линейная S-образная функция принадлежности нечеткого множества $A_{\text{В}}^{v} = \{\mu_{\text{В}}^{v}(x)/x\}$, соответствующего нечеткой переменной «В» для лингвистической переменной P_γ:

$$\mu_{B}^{v}(x;c,d) = \begin{cases} 0, & x \le c, \\ \dfrac{x-c}{d-c}, & c < x < d, \\ 1, & d \le x. \end{cases} \tag{10}$$

На рис. 5 представлены три графика функций принадлежности нечетких переменных, используемых для задания лингвистической переменной – вероятность использования уязвимости P_γ.

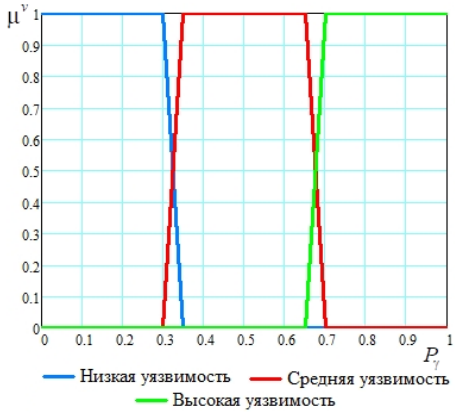

Рис. 5. Графики функции принадлежности нечетких множеств $A_{\text{Н}}^{v}$, $A_{\text{С}}^{v}$, $A_{\text{В}}^{v}$

Эксперт на основании априорных знаний присваивает лингвистические значения, представляющие собой наименования нечетких переменных, для каждой вероятности использования уязвимости P_γ как компоненты соответствующего барьера b_l, благодаря которой становится возможной реализация соответствующей угрозы t_i. Эти значения представляются вербально как: «Н», «С», «В». Так как с каждым таким значением связывается соответствующая функция принадлежности с соответствующими приблизительными количественными оценками, то для каждой уязвимости γ_ψ можно вычислить с ограниченной степенью точности численное значение этой вероятности P_{γ_ψ}, например, как модальное значение соответствующего нечеткого множества.

По аналогии можно определить степень сопротивляемости средств защиты (называемых в литературе [8, 11, 12, 45 – 48] также как механизмы, меры, средства контроля (англ. controls), к которым относится любой процесс, политика, устройство, установившаяся практика или другие действия, которые изменяют риск [11]), характеризующуюся вероятностью их преодоления ($P_l^{ov} = 1 - R_l$). Соответствующие уровни контроля (степень сопротивляемости) могут быть определены следующим образом:

– В – высокая степень сопротивляемости средства (меры, механизма) защиты (высокий уровень контроля). Маловероятно, что такой механизм удастся преодолеть. Вероятность преодоления (обхода) такого механизма находится в диапазоне – $P_l^{ov} \in [0,\ 0.4]$;

– С – средняя степень сопротивляемости средства защиты. Такое средство (мера) обеспечивает определенную защиту, однако есть возможность его преодолеть, затратив определенные усилия. Вероятность преодоления соответствующей меры защиты находится в диапазоне [0.4, 0.8];

– Н – низкая степень сопротивляемости средства защиты. Такое средство (меру) довольно просто преодолеть. Вероятность преодоления соответствующей меры защиты находится в диапазоне [0.8, 1].

Тогда, воспользовавшись этой шкалой, определим наименования нечетких переменных (δ_ε, где $\varepsilon \in \square^*_{<n}$) – множество значений терм-множества T_R лингвистической переменной R: T_R ={«высокая степень сопротивляемости», «средняя степень сопротивляемости», «низкая степень сопротивляемости»}={«В», «С», «Н»}, то есть δ_1=«В», δ_2 =«С», δ_3=«Н». Областью определения каждой из нечетких переменных является множество числовых значений ($X \in [0,1]$) вероятности преодоления средств защиты. В рассматриваемом случае также ограничимся предположением о тривиальном характере G_R и M_R (без логических связок и модификаторов).

Подобно приведенному выше подходу для рассматриваемых нечетких переменных δ_1=«В», δ_2 = «С», δ_3=«Н» (с которыми связываются соответствующие нечеткие множества, определяющие их возможные значения: $A_{\text{Н}}^{ov} = \{\mu_{\text{Н}}^{ov}(x)/x\}$, $A_{\text{С}}^{ov} = \{\mu_{\text{С}}^{ov}(x)/x\}$, $A_{\text{В}}^{ov} = \{\mu_{\text{В}}^{ov}(x)/x\}$) были выбраны трапециевидная, линейная Z- и линейная S-образные функции принадлежности ($\mu_{\text{Н}}^{ov}(x)$, $\mu_{\text{С}}^{ov}(x)$, $\mu_{\text{В}}^{ov}(x)$). На рис. 6 представлены три графика функций принадлежности нечетких переменных, используемых для определения лингвистической переменной, – степени сопротивляемости средства защиты R ($R = 1 - P^{ov}$; в некоторых источниках [45] P^{ov} называют обратной силой контроля (англ. reverse of the control strength)).

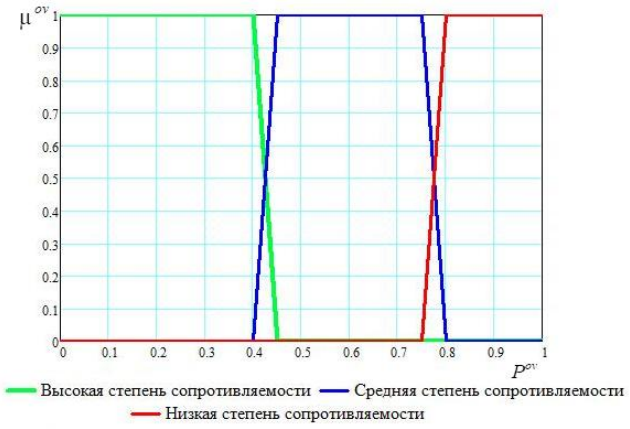

Рис. 6. Графики функции принадлежности нечетких множеств $A_{\text{Н}}^{ov}$, $A_{\text{С}}^{ov}$, $A_{\text{В}}^{ov}$

Эксперт на основании априорных знаний об используемых средствах защиты (защитных мерах), затрудняющих использование соответствующей уязвимости γ_ψ, благодаря которой становится возможной реализация соответствующей угрозы t_i, присваивает лингвистические значения «высокая степень сопротивляемости», «средняя степень сопротивляемости», «низкая степень сопротивляемости» или «В», «С», «Н» для каждой R_l как компоненты соответствующего барьера b_l. Ввиду того, что с каждым таким значением связывается соответствующая функция принадлежности с соответствующими приблизительными количественными оценками, то для каждого средства обеспечения безопасности $w_k \in W$ барьера b_l можно определить численное значение как P_l^{ov}, так и $R_l = 1 - P_l^{ov}$. Опять же, как модальное значение соответствующего нечеткого множества.

Ущерб (как убыток, урон, потеря), причиняемый в результате инцидентов безопасности, связывается с целевой функцией системы – одним из соответствующих показателей, таким как упущенная выгода, потеря конкурентных преимуществ, ухудшение репутации организации, причинение вреда интересам третьей стороны, финансовые потери, связанные с восстановлением ресурсов, дезорганизация деятельности в связи с недоступностью данных и т. д. Для разных организаций важность каждого из них может иметь существенно разное значение.

С экономической точки зрения ущерб активам удобно представлять в терминах финансовых потерь. Однако на практике получение точных количественных значений ущерба часто затруднено или вообще невозможно [10]. Тем не менее, большинство не поддающихся количественному описанию потерь можно представить в численном виде путем использования эмпирической шкалы уровня ущерба – качественной шкалы измерения, разделенной на области (ранги), соответствующие различным степеням удовлетворения рассматриваемых требований, например, пятибалльной шкалы: от 1 до 5. Каждому из таких уровней (рангов) можно сопоставить значение терм-множества T_L (T_L={«Очень низкий», «Низкий», «Средний», «Высокий», «Очень высокий»}={«VL», «L», «M», «H», «VH»}) лингвистической переменной – величина ущерба L. Областью определения каждой из нечетких переменных является множество числовых значений величины ущерба/уровня ущерба (в баллах) $X \in (0,6)$. В рассматриваемом случае можно ограничиться предположением о тривиальном характере G_L и M_L.

Для рассматриваемых нечетких переменных ρ_1=«VH», ρ_2=«H», ρ_3=«M», ρ_4=«L», ρ_5=«VL» (с которыми связываются соответствующие нечеткие множества, определяющие их возможные значения: $A_{\text{VH}}^L = \{\mu_{\text{VH}}^L(x)/x\}$, $A_{\text{H}}^L = \{\mu_{\text{H}}^L(x)/x\}$, $A_{\text{M}}^L = \{\mu_{\text{M}}^L(x)/x\}$,

$A_{\text{L}}^{L}=\{\mu_{\text{L}}^{L}(x)/x\}$, $A_{\text{VL}}^{L}=\{\mu_{\text{VL}}^{L}(x)/x\}$) были выбраны треугольные, линейная Z- и линейная S-образные функции принадлежности ($\mu_{\text{VH}}^{L}(x)$, $\mu_{\text{H}}^{L}(x)$, $\mu_{\text{M}}^{L}(x)$, $\mu_{\text{L}}^{L}(x)$, $\mu_{\text{VL}}^{L}(x)$):

$$\mu_{\text{VL}}^{L}(x;a,b)=\begin{cases}1, & x\le a,\\ \dfrac{b-x}{b-a}, & a<x<b,\\ 0, & b\le x,\end{cases}\qquad \text{где } a=1;\ b=2. \tag{11}$$

– $$\mu_{\text{H}}^{L}(x;a,b,c,d),\mu_{\text{M}}^{L}(x;a,b,c,d),\mu_{\text{L}}^{L}(x;a,b,c,d)=\begin{cases}0, & x\le a,\\ \dfrac{x-a}{b-a}, & a\le x\le b,\\ \dfrac{c-x}{c-b}, & b\le x\le c,\\ 0, & c\le x,\end{cases} \tag{12}$$

где для μ_{H}^{L} a=1, b=2, c=3; для μ_{M}^{L} a=2, b=3, c=4; для μ_{L}^{L} a=3, b=4, c=5;

– $$\mu_{\text{VH}}^{L}(x;c,d)=\begin{cases}0, & x\le c,\\ \dfrac{x-c}{d-c}, & c<x<d,\\ 1, & d\le x,\end{cases}\qquad \text{где } c=4;\ d=5. \tag{13}$$

На рис. 7 представлены графики функций принадлежности нечетких переменных, используемых для задания лингвистической переменной – величина ущерба L.

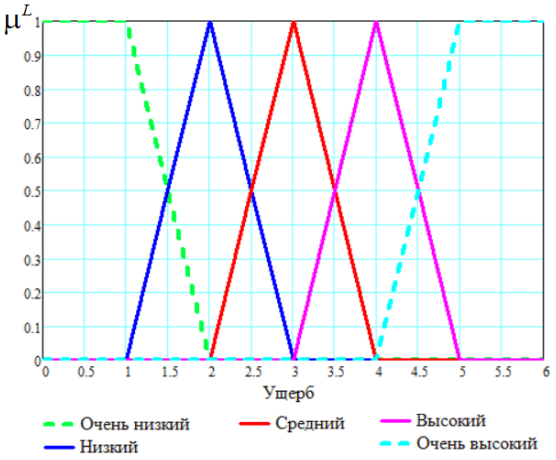

Рис. 7. Графики функции принадлежности нечетких множеств A_{VH}^{L}, A_{H}^{L}, A_{M}^{L}, A_{L}^{L}, A_{VL}^{L}

В табл. 1 представлена оценка величины ущерба в пятибалльной шкале и его семантическая характеристика.

Таблица 1

Уровень ущерба	**Значение терм-множества T_L**	**Семантическая характеристика значения показателя величины ущерба**
1	Очень низкий	Ущербом можно пренебречь.
2	Низкий	Ущерб легко устраним, затраты на ликвидацию последствий реализации угрозы невелики.
3	Средний	Ликвидация последствий реализации угрозы не связана с крупными затратами.
4	Высокий	Ликвидация последствий реализации угрозы связана со значительными финансовыми потерями.
5	Очень высокий	Организация прекращает существование.

Для того чтобы оценка ценности активов имела экономический смысл, качественную шкалу оценки ущерба целесообразно соотнести с размером прямых финансовых потерь. Однако установление такого соответствия требует дополнительных исследований в каждом конкретном случае и зависит от многих факторов для рассматриваемых систем. Возможная шкала оценки прямых финансовых потерь может выглядеть подобно той, что показана в табл. 2. Все зависит от задач, решаемых организацией, областью, характером и масштабами ее деятельности, формой собственности, стоимости активов, тяжести последствий нарушения их безопасности и ряда других факторов.

Таблица 2

Уровень ущерба	**Значение терм-множества T_L**	**Финансовые потери**
1	Очень низкий	менее 100 $
2	Низкий	(100-1000) $
3	Средний	(1000-10 000) $
4	Высокий	(10 000-100 000) $
5	Очень высокий	свыше 100 000 $

Таким образом, располагая соответствующими данными, воспользовавшись выражением (2), можно определить величину защищенности анализируемой БД.

Выводы

1. Исходя из анализа и обобщения различных подходов и достижений в области оценки безопасности информационных систем в целом и баз данных в частности было принято решение модель защиты БД и ее оценку строить на основе известной модели системы безопасности с полным перекрытием, опирающуюся на теорию графов, нечетких множеств, вероятностей, и традиционно считающуюся основой формального описания систем защиты.

2. В результате формализации задачи обеспечения безопасности баз данных:

– определены основные объекты защиты реляционных БД (с учетом двойственной природы системы БД и различной степени детализации ее компонент);

– выявлены основные значимые антропогенные угрозы безопасности баз данных;

– определен (на основе анализа существующих таксономий) перечень основных общих слабых мест (недостатков) как некоторых типов уязвимостей;

– определен показатель защищенности БД (эффективности/результативности безопасности) как величина обратная суммарному остаточному риску, составные компоненты которого представляются в виде соответствующих лингвистических переменных.

3. Разработан метод оценивания основных компонент барьеров безопасности и защищенности базы данных в целом, опирающийся на теорию нечетких множеств и риска.

4. Предлагаемая модель защиты, в которой в явном виде учитывается понятие уязвимости как отдельно объективно существующей категории (слабого места актива или средства управления, которое может быть использовано одной или более угрозой), что позволяет более адекватно оценивать вероятность нежелательного инцидента (реализации угрозы) в двухфакторной модели (в которой один из факторов отображает мотивационную составляющую возникновения угрозы, а второй учитывает существующие уязвимости), а следовательно, и оценку защищенности БД в целом, является дальнейшим развитием модели Клементса – Хоффмана.

Список литературы:

1. ISO/IEC 25010:2011 Systems and software engineering. Systems and software Quality Requirements and Evaluation (SQuaRE). System and software quality models. URL: https://www.iso.org/standard/35733.html/. (accessed on 12 August 2021).
2. Смирнов С. Н. Безопасность систем баз данных. Москва : Гелиос АРВ, 2007. – 352 с.
3. Tanenbaum A. S., Bos H. Modern Operating Systems. Fourth edition. Pearson, 2015. 1136 p.
4. Хоффман, Л. Дж. Современные методы защиты информации. Москва : Сов. радио, 1980. 264 с.

5. Hoffman L. J., Clements D. Fuzzy computer security metrics: A preliminary report. Memorandum No. ERL-M77/6 27 January 1977. Electronics research laboratory. College of Engineering University of California, Berkeley. 20 p. https://www2.eecs.berkeley.edu/Pubs/TechRpts/1977/ERL-m-77-6.pdf. (accessed on 12 August 2021).
6. Committee on National Security Systems (CNSS) Glossary. CNSSI No. 4009, 2015. URL: h https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf. (accessed on 12 August 2021).
7. Щербаков А. Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. Москва : Книжный мир, 2009. 352 с.
8. Астахов А. Анализ защищенности корпоративных систем // Открытые системы. 2002. № 7-8. URL: https://www.osp.ru/os/2002/07-08/181720. (accessed on 12 August 2021).
9. Аверченков В. И., Рытов М. Ю., Гайнулин Т. Р. Оптимизация выбора состава средств инженерно-технической защиты информации на основе модели Клементса – Хоффмана // Вестн. Брянск. гос. техн. ун-та. 2008. № 1(17). С. 61-66.
10. Карпычев В. Ю. Экономический анализ нормативно-технического обеспечения информационной безопасности // Экономический анализ: теория и практика. 2011. №35 (242). С. 2-18.
11. ISO/IEC 27000:2018 Information technology. Security techniques. Information security management systems. Overview and vocabulary. URL: https://www.iso.org/standard/73906.html. (accessed on 12 August 2021).
12. Астахов А. М. Искусство управления информационными рисками. Москва : ДМК Пресс, 2010. 312 с.
13. Скиба А. В., Архипов А. Е. Информационные риски: модели рисков, исследование и использование // Інвестиції: практика та досвід. 2016. № 1. С. 51-60.
14. Архипов А. Е. Экспертно-аналитическое оценивание информационных рисков и уровня эффективности системы защиты информации // Радіоелектроніка. Інформатика. Управління. 2009. № 2. С. 111-115.
15. DB-Engines Ranking. URL: https://db-engines.com/en/ranking. (accessed on 12 August 2021).
16. TOPDB Top Database index. URL: https://pypl.github.io/DB.html. (accessed on 12 August 2021).
17. Gartner, Magic Quadrant for Operational Database Management Systems, Merv Adrian, Donald Feinberg, Nick Heudecker, 25 November 2019 – ID G00376881. URL: https://www.gartner.com/en/documents/3975492/magic-quadrant-for-operational-database-management-syste. (accessed on 12 August 2021).
18. Critical Capabilities for Cloud Database Management Systems for Operational Use Cases. Published 24 November 2020 – ID G00468197. Merv Adrian, Donald Feinberg, Rick Greenwald, Adam Ronthal, Henry Cook, https://www.oracle.com/explore/adw-ocom/gartner-cloud-database-management/?source=:ow:o:p:mt:::RC_WWMK200720P00100:Gartnerdatabase&intcmp=:ow:o:p:mt:::RC_WWMK200720P00100:Gartnerdatabase&lb-mode=overlay; https://www.oracle.com/database/gartner-dbms.html. (accessed on 12 August 2021).
19. Sandhu R. S., Jajodia S. Data and database security and controls // Handbook of information security management, Auerbach Publishers. 1993. P. 481-499.
20. Groff J., Weinberg P., Oppel A. SQL. The Complete Reference. 3rd ed. New York, NY, USA: McGraw-Hill, Inc.; 2010. – 912 p.
21. Муханова А., Ревнивых А. В., Федотов А. М. Классификация угроз и уязвимостей информационной безопасности в корпоративных системах // Вестн. Новосибир. гос. ун-та. Сер.: Информационные технологии. 2013. Т. 11, № 2. С. 55-72.
22. Kulkarni S., Urolagin S. Review of attacks on databases and database security techniques // International Journal of Emerging Technology and Advanced Engineering. 2012. Vol. 2, Issue 11. P. 2250-2459.
23. Rohilla S., Mittal P. K. Database Security: Threads and Challenges // International Journal of Advanced Research in Computer Science and Software Engineering. 2013, Vol. 3, Issue 5. P. 810–813.
24. Pfleeger C. P., Pfleeger S. L., Margulies J. Security in Computing. Fifth Edition. Prentice Hall. 2015. 944 p.
25. Imperva Whitepaper. Top ten database security threats. 2015. – URL: https://files.meetup.com/5631682/WP_TopTen_Database_Threats.pdf. (accessed on 12 August 2021).
26. Imperva Whitepaper. Top 5 Database Security Threats. 2016. URL: https://www.imperva.com/docs/gated/WP_Top_5_Database_Security_Threats.pdf. (accessed on 12 August 2021).
27. Вілігура В. В. Систематизація загроз і вразливостей характерних для баз даних і СУБД // Праці 7-ої Міжнар. конф. «Комп'ютерне моделювання в наукоємних технологіях (КМНТ-2021), 21-23 квітня 2021 р. Харків : Харк. нац. ун-т імені В. Н. Каразіна, 2021. С. 83-86.
28. MITRE. CVE. Common Vulnerabilities and Exposures. URL: https://cve.mitre.org/data/downloads/allitems.html. (accessed on 12 August 2021).
29. MITRE. CWE Version 4.2. 2020-08-20. URL: https://cwe.mitre.org/data/published/cwe_v4.2.pdf. (accessed on 12 August 2021).
30. MITRE. Common Weakness Enumeration. CWE List Version 4.2. URL: https://cwe.mitre.org/data/index.html. (accessed on 12 August 2021).
31. ГОСТ Р 56546-2015 Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем. URL: https://docs.cntd.ru/document/1200123702. (accessed on 12 August 2021).
32. Марков А. С., Фадин А. А. Систематика уязвимостей и дефектов безопасности программных ресурсов // Защита информации. Инсайд. 2013. № 3. С. 2-7.

33. MITRE. CWE VIEW: Research Concepts. URL: https://cwe.mitre.org/data/definitions/1000.html. (accessed on 12 August 2021).
34. Zadeh L. A. The concept of a linguistic variable and its application to approximate reasoning – I // Information sciences. 1975. Vol. 8, Issue 3. P. 199-249.
35. NIST Special Publication 800-30 Revision 1. September 2012. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf. (accessed on 12 August 2021).
36. Нестеров С. А. Анализ и управление рисками в информационных системах на базе операционных систем Microsoft. Москва : Национальный Открытый Университет "ИНТУИТ", 2016. 251 с.
37. Петренко С. А., Симонов С. В. Управление информационными рисками. Экономически оправданная безопасность. Москва : Академия АйТи : ДМК Пресс, 2004. – 384 с.
38. Корниенко А. А., Никитин А. Б., Диасамидзе С. В., Кузьменкова Е. Ю. Моделирование компьютерных атак на распределенную информационную систему // Изв. Петербург. ун-та путей сообщения. 2018. Т. 15. № 4. С. 613-628.
39. Talabis M., Martin J. Information Security Risk Assessment Toolkit Practical Assessments through Data Collection and Data Analysis. Waltham, MA, USA : Syngress, 2012. 258 p.
40. Hajek A. Interpretations of probability. In The Stanford Encyclopedia of Philosophy. URL: https://plato.stanford.edu/entries/probability-interpret/. (accessed on 12 August 2021).
41. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. 2008. URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/380-metodika-opredeleniya-aktualnykh-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-fstek-rossii-2008-god. (accessed on 12 August 2021).
42. Леоненков А. В. Нечеткое моделирование в среде MATLAB и fuzzyTECH. СПб. : БХВ Петербург, 2005. 736 с.
43. Круглов В. В., Дли М. И., Голунов Р. Ю. Нечеткая логика и искусственные нейронные сети. Москва : Физматлит, 2001. 201 с.
44. Piegat A. Fuzzy Modeling and Control. Heidelberg ; New York: Physica-Verlag, 2001. 733 p.
45. Talabis M., Martin J. Information Security Risk Assessment Toolkit Practical Assessments through Data Collection and Data Analysis. Waltham, MA, USA : Syngress, 2012. 258 p.
46. Whitman M. E., Mattord H. J. Principles of Information Security, 6th Edition. Boston, MA, USA : Cengage Learning, 2017. 656 p.
47. NIST Special Publication 800-53 Revision 5. (2020). Security and Privacy Controls for Information Systems and Organizations. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf. (https://doi.org/10.6028/NIST.SP.800-53r5). (accessed on 12 August 2021).
48. ISO/IEC 27002:2013 Information technology. Security techniques. Code of practice for information security controls. URL: https://www.iso.org/standard/54533.html. (accessed on 12 August 2021).

Поступила в редколлегию 22.09.2021

Сведения об авторах:

Вилигура Владислав Викторович – аспирант, Харьковский национальный университет имени В.Н. Каразина, кафедра безопасности информационных систем и технологий, факультета компьютерных наук; Украина; e-mail: viligura93@gmail.com; ORCID: https://orcid.org/0000-0002-1137-2382

Есин Виталий Иванович – д-р техн. наук, доцент, Харьковский национальный университет имени В.Н. Каразина, профессор, кафедра безопасности информационных систем и технологий, факультета компьютерных наук; Украина; e-mail: v.i.yesin@karazin.ua; ORCID: https://orcid.org/0000-0003-1977-7269