И. В. Машкина, А. Ю. Сенцова

МЕТОДОЛОГИЯ ЭКСПЕРТНОГО АУДИТА В СИСТЕМЕ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ[1]

Облачные вычисления — инновационная технология, которая предоставляет динамично масштабируемые вычислительные ресурсы и приложения через Интернет в качестве сервиса под управлением поставщика услуг [1].

Облачные вычисления с точки зрения информационной безопасности имеют несколько существенных особенностей, которые обусловлены слабо проработанными стандартами безопасности в данной области, отсутствием анализа статистики по инцидентам в облаках, а также тем, что сохранность пользовательских данных практически в полной мере зависит от компании-провайдера облачных сервисов — вендора.

Данная работа посвящена проблеме аудита информационной безопасности (ИБ) в системе облачных вычислений (СОбВ), под которой понимается информационная система взаимодействия вендора и заказчика услуг.

Информационная безопасность в системе облачных вычислений может быть определена как создание таких условий информационного взаимодействия заказчика и вендора, при которых обеспечивается защищенность СОбВ от угроз нарушения конфиденциальности и целостности циркулирующей в системе, обрабатываемой в инфраструктуре вендора информации, а также от угроз нарушения доступности сервиса. При этом предотвращение угроз нарушения доступности облачных сервисов должно обеспечиваться исключением единой точки сбоя известными методами.

Обеспечение режима информационной безопасности при разумных вложениях является серьезной актуальной проблемой для поставщика облачных сервисов. Как оценить уровень риска нарушения безопасности информации, который обеспечивается вендором при предоставлении заказчику облачных услуг? Какие ответные действия по реагированию на инциденты будут рациональными, то есть минимизирующими ущерб вендора и заказчика услуг? Эти вопросы возникают как при проектировании системы обеспечения информационной безопасности (СОИБ) инфраструктур вендора и клиента, так и в процессе функционирования СОбВ.

Оценка степени соответствия компонентов СОИБ требованиям существующих стандартов в области ИБ, построение модели угроз, оценка рисков и разработка рекомендаций по их управлению осуществляются в ходе проведения экспертного аудита.

Состояние безопасности использования заказчиком облачных сервисов может быть оценено величиной уровня риска нарушения информационной безопасности $\overline{R}$. Если $\overline{R} \le \overline{R}_{доп}$, где $\overline{R}_{доп}$ – значение допустимого уровня риска, то защищенность информации в СОбВ соответствует требованиям заказчика.

[1] Работа выполнена при поддержке гранта РФФИ № 14-07-00928-а.

В международных и российских стандартах в области информационной безопасности сформированы требования к *методологии оценивания рисков* нарушения ИБ [2]. Методология должна обеспечивать получение численных значений уровня риска, помогать осуществлять внутренний *аудит* для обоснования выбора корректирующих действий в процессе менеджмента защиты информации, обеспечивать способность к быстрой адаптации при изменении компонентов инфраструктуры, должна гарантировать, что метод оценки рисков дает сравнимые и сопоставимые результаты.

В настоящее время в России нет стандартов, на основе которых можно строить решения по информационной безопасности для облачных технологий [3]. В США ассоциация Cloud Security Alliance выпустила Cloud Controls Matrix. Этот документ представляет собой перечень существующих технологий информационной безопасности, которые могут быть использованы в облачных сервисах [4]. Хотя некоторые специалисты считают, что для управления ИБ при построении облака SaaS могут быть использованы стандарты ISO 27001 и ISO 27002 [5], все же необходима разработка специальных стандартов для облачных вычислений.

Что касается рекомендаций и методик оценивания рисков нарушения ИБ в системе облачных вычислений, то они отсутствуют не только в нормативной базе РФ, но и в законодательных актах других стран [6].

Поэтому рассматриваемая в данной работе тематика исследований, направленных на развитие методологии управления информационными рисками в системе облачных вычислений, является актуальной.

Научная проблема получения численного значения риска нарушения ИБ, заключающаяся в выявлении функциональной зависимости значения уровня риска от характеристик компонентов инфраструктуры с учетом сетевой топологии объекта защиты, от параметров имеющихся барьеров, а также от ценности обрабатываемой информации, была решена в работах [7, 8].

В [7, 8] авторам удалось преодолеть чрезмерную сложность и трудноформализуемость проблемы и разработать метод оценивания риска нарушения ИБ, удовлетворяющий в полной мере требованиям стандартов, численно определить влияющие на результат решения входные переменные: вероятности реализации угроз и ценность информационных ресурсов.

Для заказчика облачных сервисов уровень риска нарушения ИБ зависит от вероятностей реализации угроз информационным активам, которые обрабатываются в исследуемый период времени в среде инфраструктуры вендора, а также от вероятностей угроз информационным ресурсам ограниченного доступа на стороне заказчика.

В данной работе предложенная методология используется применительно к системе облачных вычислений для расчетов прогнозируемых численных значений уровней рисков в СОбВ в процессе экспертного аудита.

В ходе экспертного аудита СОбВ важно оценить не только значение уровня риска нарушения информационной безопасности с учетом всего перечня потенциально возможных угроз, но и *оперативное* значение риска, когда угроза проявляется по конкретному пути распространения. Для оценки оперативного значения уровня риска нарушения информационной безопасности, связанного с появлением угрозы в реальном масштабе времени, в работе предложено использовать искусственную нейронную сеть (ИНС).

Однако сегодня главной проблемой использования искусственной нейронной сети является формирование множества данных обучающей выборки, достаточной для обучения ИНС. Используя результаты количественной оценки прогнозируемых значений рисков нарушения информационной безопасности, рассчитанных для СОбВ, можно сформировать массив данных обучающей выборки для настройки ИНС. Сложность решения рассматриваемой проблемы обусловлена также необходимостью учета изменяющегося параметра «ценность информации».

В работе для преодоления этой сложности обоснована целесообразность настройки ИНС по значениям этого параметра.

Оценить риск нарушения информационной безопасности без учета особенностей инфраструктуры объекта защиты в общем виде невозможно. Поэтому на основе анализа известных технологий клиент-серверного взаимодействия в работе предложен возможный вариант архитектуры СОбВ, представленный на рис. 1, где: R – маршрутизатор, F – межсетевой экран, AN – антивирус, OS – операционная система, App – приложение, web – web-сервер, Blade – Blade-сервер, FTP – файловый сервер, DNS – DNS-сервер.

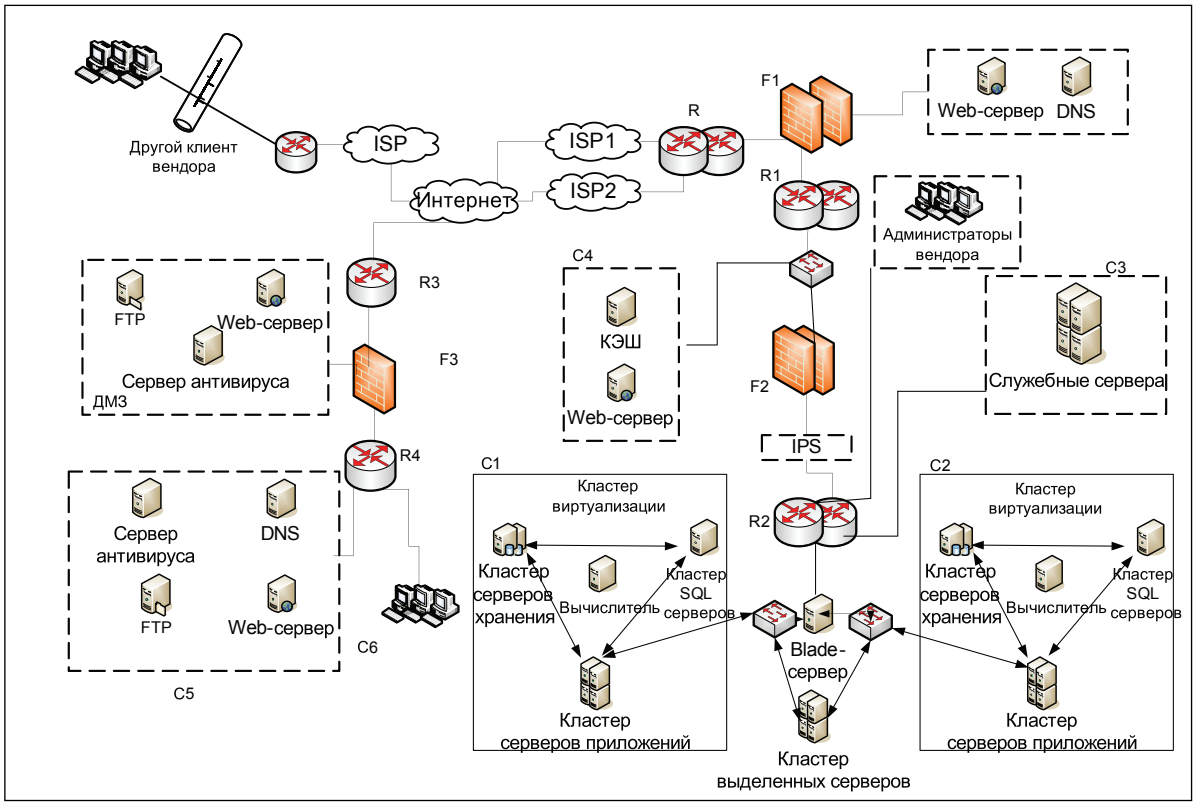

Рис. 1. Архитектура СОбВ

При разработке варианта инфраструктуры СОбВ учтены требования архитектуры безопасности. Типовая архитектура *демилитаризованной зоны* включает в себя: публичный web-сервер, обеспечивающий доступ из сети Интернет любого пользователя к информационным ресурсам портала, DNS-сервер, сервер приложений для управления информационными ресурсами web-портала. Вендор использует web-портал в качестве рекламы в сети Интернет своей деятельности по предоставлению облачных сервисов. В демилитаризованной зоне должна храниться и обрабатываться только общедоступная открытая информация.

Чтобы минимизировать риски заказчика и вендора в процессе реализации облачных сервисов, внутренний web-сервер для клиент-серверного взаимодействия должен быть размещен в другом сетевом сегменте, как и КЭШ-сервер, обеспечивающий временное хранение ресурсов клиентов облачных сервисов и позволяющий уменьшить время доступа пользователей к кэшированным данным. То есть следует обеспечить сегрегацию этих серверов от общедоступных, располагая их во внутренней защищенной подсети вендора.

Основа облачной инфраструктуры – кластер виртуализации и кластер выделенных серверов – также находятся во внутренней защищенной подсети. Кроме того, здесь же расположены

кластеры серверов системы хранения данных и кластер SQL-серверов. Особое внимание уделяется взаимной защите между виртуальными машинами.

Для решения проблемы управления рисками нарушения ИБ в СОбВ необходимо идентифицировать внешние и внутренние факторы, влияющие на риск, и произвести оценивание уровня риска в количественном выражении. В рамках данной работы при оценивании риска нарушения ИБ в СОбВ во внимание предлагается принимать угрозы *несанкционированного доступа*, в результате которых происходит получение информации заинтересованным субъектом (злоумышленником или пользователем, нарушающим свои права), а также угрозы *утечки* — угрозы нарушения политики безопасности суперпользователем, когда сотрудник вендора, обладающий высокими привилегиями, передает по коммуникационным каналам информацию недоверенному субъекту.

Любая реализация СОИБ — это схема, содержащая в себе требования к защите и *модель угроз*, отражающую защищаемую среду и состояние оборонительных барьеров.

При решении проблемы оценивания рисков нарушения ИБ в СОбВ предложено осуществить идентификацию угроз, реализуемых за счет использования уязвимостей компонентов инфраструктуры и сервисов безопасности, и произвести детализацию активов до уровня совокупности информационных ресурсов заказчика, обрабатываемых в локальных сетевых сегментах вендора и на стороне заказчика.

В работе модель угроз строится в виде нечетких когнитивных карт (НКК), представленных на рис. 2 и 3, для угроз несанкционированного доступа. Нечеткие когнитивные карты были разработаны с учетом всех возможных источников угроз и компонентов инфраструктуры СОИБ СОбВ, расположенных на путях распространения атак. При формировании модели угроз во внимание принимаются следующие особенности организации СОбВ: доступ администратора вендора к серверам и приложениям, а также уязвимости внутри виртуальной среды.

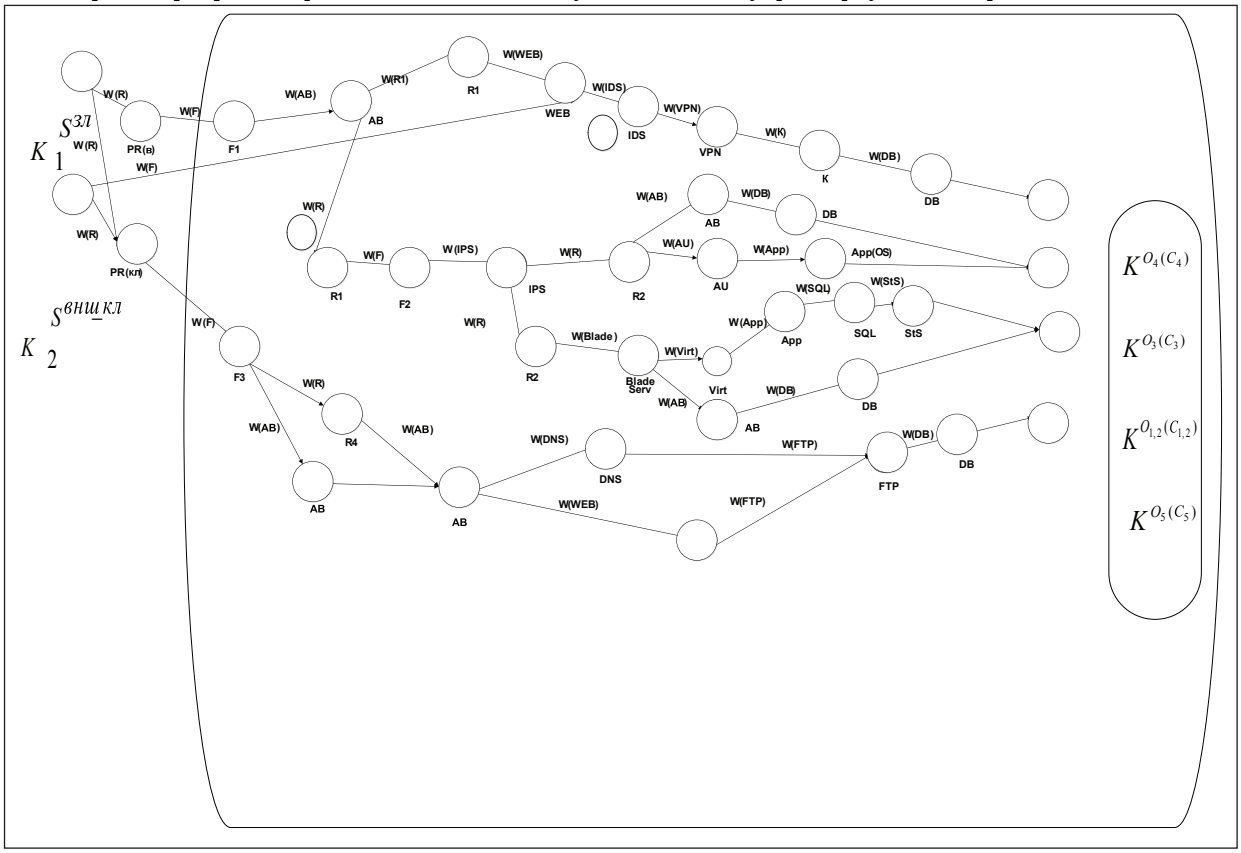

Рис. 2. НКК1 — Модель внешних угроз несанкционированного доступа

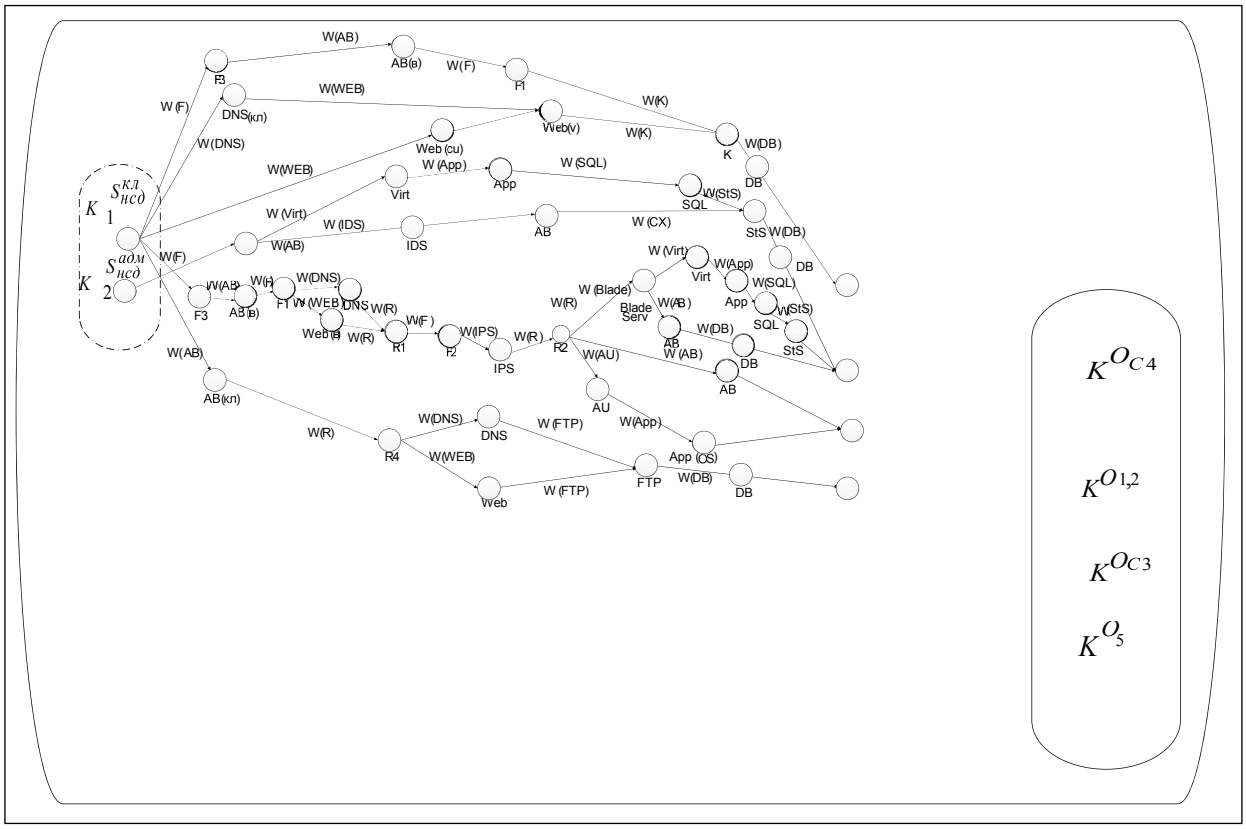

Рис. 3. НКК2 — Модель внутренних угроз несанкционированного доступа

На рис. 2 и 3 источники угроз обозначены: $S^{ЗЛ}$ – злоумышленник — несанкционированный субъект доступа (или запущенный им процесс); $S^{внш\_кл}$ – другой клиент вендора (или запущенный им несанкционированный процесс); $S_{нсд}^{адм}$ – нарушитель политики безопасности — сотрудник или администратор вендора; $S_{нсд}^{кл}$ – сотрудник заказчика; объекты атак обозначены: O_{C1} и O_{C2} – защищаемые информационные ресурсы основного и резервного кластера виртуализации; O_{C3} – информационные ресурсы в серверном сегменте вендора; O_{C4} – информационные ресурсы КЭШ-сервера; O_{C5} – информационные ресурсы в серверном сегменте на стороне компании заказчика; W – уровни уязвимостей. Промежуточные концепты НКК отображают множество компонентов инфраструктуры (сервисы безопасности, коммуникационное оборудование, программное обеспечение), находящихся на путях распространения угроз.

Когнитивная карта иллюстрирует возможные пути угроз, реализуемых потенциальным злоумышленником и нарушителем, позволяет провести анализ несанкционированного проникновения к информационным ресурсам: показывает, откуда проводится атакующее воздействие, какие узлы могут являться целями проведения атак, какими средствами защищена информационная система, какие уязвимости могут быть использованы во время атаки.

Модель угроз в СОбВ, разработанная на основе построения нечетких когнитивных карт, адекватна объекту защиты и позволяет обеспечить оценку уровней угроз. Преимуществом использования НКК в данном приложении в сравнении с какими-либо другими методами является возможность учесть инфраструктуру СОбВ, организовать знания об особенностях распространения угроз в СОбВ, а также формализовать численно не измеримые факторы, такие как вероятности угроз.

В процессе аудита вычисляются значения рисков нарушения информационной безопасности активов, обрабатываемых в сегментах инфраструктуры вендора и заказчика, в зависимости от

ценности обрабатываемой информации и оценки значимости угроз от множества источников к сегментам по следующей схеме:

- значения уровней угроз на путях распространения от одного источника к одному объекту атаки определяются как произведение вероятности активизации угрозы и полученных нормированием приведенных в международной базе данных величин уязвимостей компонентов инфраструктуры и барьеров

$$P_j = P_{акт} \cdot \prod_{z \in Z} W_{z,z+1}; \quad (1)$$

- выявляется максимальное значение уровня угрозы от источника к объекту атаки

$$P_S^U(K_i \to K_y) = \max_{j=1}^{J} P_j, \quad (2)$$

где J — число путей от одного источника к одному объекту;

- аналогичные вычисления проводятся для всех возможных источников угроз информационным активам сегмента;

- для вычисления результирующего значения уровня угрозы информационным активам сегмента используем формулу:

$$P_\Sigma^U = 1 - \Pi\left(1 - P_S^U\right); \quad (3)$$

- расчеты проводятся для каждого сегмента;

- значение уровня риска нарушения ИБ информационных активов сегмента:

$$\overline{R}_n = \sum_{s=1}^{S} P_\Sigma^U \cdot \frac{Ц_s}{Ц_\Sigma}, \quad (4)$$

где S — число источников угроз;

- результирующее значение риска нарушения ИБ в СОбВ определяется по формуле:

$$\overline{R} = \sum_{n=1}^{N} \overline{R}_n, \quad (5)$$

где N — число анализируемых сегментов.

Метод позволяет получить оценку значения уровня риска нарушения ИБ для *наихудшего случая*, когда одновременно активизируются все возможные источники угроз.

Кроме того, значение уровня риска является функцией ценности активов, обрабатываемых в СОбВ. Следует заметить, что значение параметра «ценность информации» не может быть получено путем какого-либо объективного измерения. Ценность информации может быть задана собственником и определяется степенью полезности или важности для него какого-либо актива. Для определения ценности информационных активов сегмента может быть использован метод, позволяющий учесть объективные сведения об обрабатываемых информационных активах: количество информационных объектов заданного уровня критичности и число возможных видов последствий для бизнеса в случае нарушения условий обеспечения защищенности [8]. Возможные виды последствий и их значимость определяются собственником информации, который может опираться в своих суждениях на рекомендации, приведенные в [9].

Поэтому при формировании множества данных обучающей выборки для ИНС в качестве входного параметра необходимо использовать кроме вероятности активизации угрозы Ра параметр «ценность информации». В таблице 1 приведен фрагмент множества данных обучающей выборки для обучения ИНС.

Таблица 1. Фрагмент множества данных обучающей выборки ИНС

Ра	С1 Кл	С2 КЭШ	С3 В	R [отн. ед.]
0	0	0	0	0
0,1	0	0	1	0,01

Ра	С1 Кл	С2 КЭШ	С3 В	R [отн. ед.]
0	0,3	0,1	0,6	0
0,1	0,3	0,1	0,6	0,02

0,2	0	0	1	0,03	0,2	0,3	0,1	0,6	0,04
…					…				
0,9	0	0	1	0,11	0,9	0,3	0,1	0,6	0,17
1	0	0	1	0,12	1	0,3	0,1	0,6	0,19
0	0	0,1	0,9	0	0	0,4	0,1	0,5	0
0,1	0	0,1	0,9	0,02	0,1	0,4	0,1	0,5	0,02
0,2	0	0,1	0,9	0,03	0,2	0,4	0,1	0,5	0,04
…					…				
0,9	0	0,1	0,9	0,14	0,9	0,4	0,1	0,5	0,18
1	0	0,1	0,9	0,15	1	0,4	0,1	0,5	0,2
0	0,1	0,1	0,8	0	0	0,5	0,1	0,4	0
0,1	0,1	0,1	0,8	0,02	0,1	0,5	0,1	0,4	0,02
0,2	0,1	0,1	0,8	0,03	0,2	0,5	0,1	0,4	0,05
…					…				
0,9	0,1	0,1	0,8	0,15	0,9	0,5	0,1	0,4	0,19
1	0,1	0,1	0,8	0,17	1	0,5	0,1	0,4	0,21
0	0,2	0,1	0,7	0	0	0,6	0,1	0,3	0
0,1	0,2	0,1	0,7	0,02	0,1	0,6	0,1	0,3	0,03
0,2	0,2	0,1	0,7	0,04	0,2	0,6	0,1	0,3	0,05
…					…				
0,9	0,2	0,1	0,7	0,16	0,9	0,6	0,1	0,3	0,2
1	0,2	0,1	0,7	0,18	1	0,6	0,1	0,3	0,23

Полученные расчетные значения прогнозируемого риска нарушения ИБ используются в качестве множества данных обучающей выборки для настройки ИНС. При выявлении пути реализации конкретной угрозы выходной слой нейронов обученной сети на основе информации с датчиков событий выдает на выходах нейронных элементов оперативное значение риска.

Модель автоматизированного средства для проведения экспертного аудита, реализующего описанную выше методику, изображена на рис. 4.

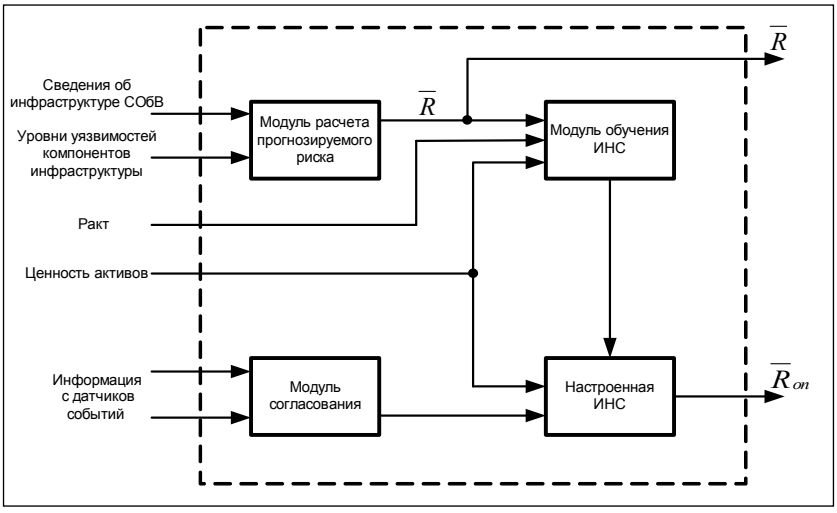

Рис. 4. Модель автоматизированной системы экспертного аудита

Результаты расчетов рисков нарушения ИБ в СОбВ при проведении экспертного аудита могут быть использованы вендором при обсуждении с заказчиком применяемых стратегий безопасности для обоснования своих возможностей по обеспечению защищенности информации заказчика и предоставления ему гарантируемых вендором показателей. Необходимость обследования уровня безопасности СОбВ возникает также в случае создания виртуального центра обработки данных в рамках собственной компании — частного облака. Кроме того, оценка риска нарушения ИБ в реальном масштабе времени позволит осуществить выбор рационального варианта реагирования на возможные инциденты.

СПИСОК ЛИТЕРАТУРЫ:

1. Облачные вычисления, «дырявые» облака и способы защиты данных [Электронный ресурс]. URL: http://www.4by4.ru/ru/analytics/oblachnye-vychisleniya-dyryavye-oblaka-i-sposoby-zashchity-dannyh.
2. ГОСТ Р ИСО/МЭК 27005-2010 «Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности».
3. *Демурчев Н. Г., Ищенко С. О.* Проблемы обеспечения информационной безопасности при переходе на облачные вычисления // Материалы XI Международной научно-практической конференции «Информационная безопасность». Ч. 1. Таганрог: Изд-во ТТИ ЮФУ, 2010.
4. Официальный сайт Cloud Security Alliance (CSA) [Электронный ресурс]. URL: https://cloudsecurityalliance.org.
5. Безопасность как головная боль облачных вычислений [Электронный ресурс]. URL: http://eopu.tu-bryansk.ru/index.php/news/46-bezopasnost-kak-golovnaya-bol-oblachnyx-vychislenij.html.
6. *Седов О.* Облака на горизонте // Директор информационной службы. 2010. № 7.
7. *Гузаиров М. Б., Машкина И. В., Степанова Е. С.* Построение модели угроз с помощью нечетких когнитивных карт на основе сетевой политики безопасности // Безопасность информационных технологий. 2011. № 2. С. 37—49.
8. *Гузаиров М. Б., Машкина И. В., Степанова Е. С.* Метод определения ценности информации с использованием аппарата нечеткой логики // Безопасность информационных технологий. 2012. № 1. С. 18—29.
9. ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения».